

# جرائم الإنترنت والحاسب الآلى

## ووسائل مكافحتها

ممدوح محمد الجنبهى

المحامى

عضو اتحاد المحامين العرب

منير محمد الجنبهى

المحامى

عضو اتحاد المحامين العرب

2004

الناشر

دار الفكر الجامعى

٣٠ ش سوتير الازاريطه - الاسكندرية

ت: ٤٨٤٣١٣٢





# جرائم الإنترنت والحاسب الآلى

## ووسائل مكافحتها

ممدوح محمد الجنبهى

المحامى

عضو اتحاد المحامين العرب

منير محمد الجنبهى

المحامى

عضو اتحاد المحامين العرب

2004

الناشر

دار الفكر الجامعى

٣٠ ش سوتير الازارطة - الاسكندرية

ت ٤٨٤٣١٣٢



## المقدمة

سبق وان أصدرنا العديد من المؤلفات في مجال القانون التجاري و العقود التجارية إلا انه و مع التقدم التكنولوجي المتوالي و الذي نعيشه منذ عقد مضى تطورت أساليب التجارة و أصبحنا نجد الآن عمليات تجارية تتم عبر شبكة الإنترنت فيما يعرفه بالتجارة الإلكترونية و ما يشمل ذلك من عقود إلكترونية و توقيع إلكتروني و مستندات إلكترونية و ما إلى ذلك من أشياء أصبحت كلها الآن إلكترونية بفضل التقدم التكنولوجي في كافة المجالات .

و عليه قد سبق و ان أصدرنا مؤلف عن التوقيع الإلكتروني و طبيته في الإثبات و الآن نقدم هذا المؤلف عن أخطار شبكة الإنترنت المتمثلة في جرائه الإلكترونية و وسائل مكافحتها .

أملين أن يجد كافة مستخدمي شبكة الإنترنت و كذلك العاملين بالقانون في مؤلفنا هذا خير المعين و نعو المساعدة الأمين

## المؤلفان

منير محمد الجنبهي

ممدوح محمد الجنبهي

## المحاميان

بالاستئناف العالي و مجلس الدولة

عضوا اتحاد المحامين العرب - <sup>أ</sup>عضوا اتحاد المحامين الأفروآسيوي

مستشاران قانونيان بالأمانة العامة للعرب الوطني الديمقراطي بالإسكندرية

مكتب / ٢١ شارع السمان - مصطفى كامل - الإسكندرية

تليفون مكتب / ٥٤٤٤٣٦٩ / ٠٣ - محمول / ٠١٢٢٦٧٩٠١٣ / ٠١٢٣٨٦٤٩٧٩



# الفصل الأول





## ماهية الإنترنت

### WHAT ABOUT THE INTERNET

يعتبر الإنترنت - الذي بدأ العمل بتاريخ ٢ / ١ / ١٩٦٩ عندما كونت وزارة الدفاع الأمريكية فريقا بحثيا من العلماء بمشروع بحثي كان موضوعه هو تشبيك الحاسبات - هو ثمرة التقدم العلمي العالمي في مجال الاتصالات و تبادل المعلومات و تعتبر شبكة الإنترنت INTERNET هي الشبكة الرئيسية التي تجتمع تحتها كافة الشبكات الأخرى أيا كان نوعها أو الغاية منها أما شبكة الإنترنت فإنها تتكون من عدد كبير جدا من الشبكات المترابطة و المتناثرة في كافة أنحاء العالم و من المعروف أن البروتوكول الذي يحكم كافة تلك الشبكات هو بروتوكول واحد هو البروتوكول المسمى ( بروتوكول تراسل الإنترنت - TCP / IP ) .

وكانت وزارة الدفاع الأمريكية قد كونت فريقا من العلماء للقيام بمشروع بحثي حول إنشاء شبكات تربط فيما بين أجهزة الحاسبات الإلكترونية COMPUTER وكان أساس البحث في هذا المشروع البحثي بجانب إنشاء الشبكات هو تجزئة الرسالة المراد إرسالها إلى موقع معين في الشبكة و من ثم يتم نقل كل جزء من تلك الأجزاء بسلك طريق مختلف عن الطريق الذي تسلكه الأجزاء الأخرى من الرسالة MESSAGE حتى تصل تلك الأجزاء جميعا ثم تتجمع ثانيا فتتكون الرسالة مرة أخرى كما كانت رسالة .

وكانت أهمية إجراء تلك الأبحاث لوزارة الدفاع الأمريكية في غاية الأهمية حيث كان ذلك في آتون الحرب التي أطلق عليها مصطلح ( الحرب الباردة ) والتي كانت قائمة على اشتدها فيما بين الاتحاد السوفيتي ( والذي تفكك إلى جمهوريات مستقلة الآن ) و الولايات المتحدة الأمريكية .

ففي حالة ما إذا تم اعتراض أي من أجزاء تلك الرسالة و دمرها الاتحاد السوفيتي فإن بقية أجزاء الرسالة تكمل طريقها إلى منطقة الوصول و من تلك الأجزاء التي استكملت طريقها يتم جمعها وبالتالي يمكن فهم فحواها و العمل بما فيها من تعليمات دون أن يكون للاعتراضات و عمليات التجسس السوفيتي أي اثر يذكر على تلك الرسائل .

ومن هنا كانت أهمية هذا المشروع البحثي و أهمية التجارب التي كانت تجرى من خلاله إلى وزارة الدفاع الأمريكية .

ثم تطور المشروع بعد ذلك إلى الاستعمال السلمي بجانب الاستعمال العسكري حيث انقسم عام ١٩٨٣ إلى شبكتين احتفظت الشبكة الأولى باسمها الأساسي ( ARPANE ) و بالغرض الأساسي الذي نشأت من اجله وهو خدمة جهاز المخابرات المركزية الأمريكية و يرمز إليها بـ ( CIA ) و سميت الشبكة الأخرى باسم ( MAIL NET ) و تلك الشبكة تم تخصيصها للاستخدامات المدنية التي خصصت للاستخدام السلمي المدني و من ثم ظهر اسم ( ENTER NET ) وفي عام ١٩٨٦ م أمكن ربط خمس مراكز للكمبيوترات العملاقة و أطلق عليها اسم ( NSF NET ) و التي أصبحت فيما بعد العمود الفقري و الأساسي لنمو و ازدهار شبكة الإنترنت في الولايات المتحدة الأمريكية ثم دول العالم اجمع بعد ذلك .

من يملك الإنترنت

## THE OWNER OF THE INTERNET

في البداية كانت الحكومة الأمريكية هي المالك لشبكة الإنترنت ثم انتقلت الملكية إلى المؤسسة القومية للعلوم ( مؤسسة أمريكية ) ألا انه في الوقت الحاضر لا

يمكن القول أن هناك مالك لشبكة الإنترنت فليس هناك مالك و إنما هناك ما يسمى بمجتمع الإنترنت و ليس هذا فقط و إنما أيضا التمويل فبعد أن كان التمويل حكوميا أصبح التمويل يأتي من القطاع الخاص ومن هنا أصبح هناك العديد و العديد من الشبكات الإقليمية ذات الغرض التجاري و التي تعرض الاستفادة من خدماتها بمقابل مالي .

### توسع الشبكة

## EXPANSION IN THE INTERNET

في عام ١٩٨٥ م كان هناك اقل من ألفي حاسب إلى مرتبط بالشبكة وفي عام ١٩٩٥ م وصل العدد إلى خمسة ملايين حاسب إلى مرتبط بالشبكة و في عام ١٩٩٧ م وصل العدد إلى ستة ملايين حاسب وهي تستخدم حوالي ثلاثمائة ألف ( SERVER ) متناثرة في كافة أرجاء العالم وبالنسبة لعدد المستخدمين فيمكن القول انه ينضم ستة و أربعين مستخدما جديدا للشبكة كل دقيقة على مستوى العالم .

و في استطلاع للرأي أجرته شبكة ( N U A ) الأمريكية قدر عدد مستخدمي شبكة الإنترنت **USERS OF THE INTERNET** عالميا في عام ١٩٨٨ م بحوالي مائة و أربعة و ثلاثين مليون مستخدم و تصدرت الولايات المتحدة الأمريكية و كندا الصدارة من حيث عدد المستخدمين الذي بلغ سبعون مليون مستخدم ( N U A . 6 / 1998 ) وفي تقرير أجرته و نشرته أيضا شبكة ( N U A ) الأمريكية و صدر بتاريخ ٢٦ / ١٠ / ٢٠٠٠ قدر أن عدد المستخدمين للشبكة في عام ٢٠٠٥ سيكون حوالي مائتان و خمسة و أربعون مليون مستخدم كما أن هذا التقرير قد قرر



أيضا أن اغلب تلك الزيادة من مستخدمي الإنترنت ستكون من خارج الولايات المتحدة الأمريكية ( N U A . 10 / 2000 ) .

على أن عمليات تطوير شبكة الإنترنت لم تتوقف DEVELOPING OF INTERNET DID NOT STOPOVER قط فقد أشار الرئيس السابق للولايات المتحدة الأمريكية ( بيل كلينتون ) إلى مشروع مستقبلي لتطوير شبكة الإنترنت أطلق عليه اسم ( الإنترنت ٢ ) ( ENTER NET 2 ) أو الجيل الثاني من الإنترنت فقال ( لابد من أن نبني الجيل الثاني من شبكة الإنترنت لتتاح الفرصة لجامعاتنا الرائدة و مختبراتنا القومية للتواصل بسرعة تزيد ألف مرة عن سرعات اليوم و ذلك لتطوير كل من العلاجات الطبية الحديثة و مصادر الطاقة الجديدة و أساليب العمل الجماعي ) .

وكانت شركة ( STAR BAND ) قد أجرت تجربة في شمال الولايات المتحدة الأمريكية عن مشروع لشبكة إنترنت بواسطة الأقمار الصناعية بلغت سرعته حوالي خمسمائة - كيلو / بايت - في الثانية الواحدة من شبكة الإنترنت إلى الحاسب الآلي COMPUTER وهو ما يعد قفزة هائلة في سرعة البث .

### خدمات شبكة الإنترنت

## SERVICES OF THE INTERNET

١ - البريد الإلكتروني ( E - MAIL )

إرسال و استقبال الرسائل بسرعة كبيرة جدا

٢ - القوائم البريدية

إنشاء و تحديث قوائم العناوين البريدية الخاصة بمجموعات من الأشخاص .



### ٣ - خدمة المجموعة الأخبارية

وهي تشبه خدمة القوائم البريدية ألا إنها تختلف في أن كل عضو يستطيع التحكم في نوع المقالات التي يريد استلامها .

### ٤ - خدمة الاستعلام الشخصي

حيث يمكن من خلال هذه الخدمة الاستعلام عن العنوان البريدي لأي شخص أو جهة تستخدم الإنترنت و المسجلين لديها .

### ٥ - خدمة المحادثات الشخصية

حيث يمكن التحدث مع طرف آخر صوتاً و صورة و كتابة

### ٦ - خدمة الدردشة الجماعية ( CHATING )

تشبه الخدمة السابقة ألا أنه وفي الغالب يمكن لأي شخص أن يدخل في المحادثة أو يستمع إليها دون اختيار الآخرين

### ٧ - خدمة نقل الملفات

( F T P ) لنقل الملفات من حاسب آلي إلى حاسب إلى آخر وهي اختصار كلمة  
( FILE TRANSFER PROTOCOL )

### ٨ - خدمة الأرشفة الإلكترونية

( ARCHIVE ) تمكن من البحث عن ملفات معينة قد تكون مفقودة في البرامج المستخدمة في حاسب المستخدم .

### ٩ - خدمة شبكة الاستعلامات الشاملة

( GOPHER ) تفيد في خدمات كثيرة كنقل الملفات و المشاركة في القوائم البريدية حيث تفهرس المعلومات الموجودة على الشبكة .

### ١٠ - خدمة الاستعلامات واسعة النطاق

( WAIS ) وهي تسمى بأسم حاسباتها الخادمة و هي أكثر دقة و فاعلية من الأنظمة الأخرى حيث تبحث داخل الوثائق أو المستندات ذاتها عن الكلمات الدالة

التي يحددها المستخدم ثم تقدم النتائج في شكل قائمة بالمواقع التي تحتوى على المعلومات المطلوبة .

١١ - خدمة الدخول عن بعد

( TEL NET ) وهى خدمة تتيح استخدام أي برامج أو تطبيقات في حاسب آلي آخر

١٢ - الصفحة الإعلامية العالمية

( WORLD WIDE WEB ) أو الويب ( WEB ) وهى تجمع كافة الموارد المتعددة التي تحتوى عليها الإنترنت للبحث عن كل ما في الشبكات المختلفة و إحضارها بالنص و الصوت و الصورة و تعد الويب ( WEB ) نظاما فرعيا من الإنترنت لكنها النظام الأعظم من الأنظمة الأخرى فهي النظام الشامل باستخدام الوسائط المتعددة

### مستلزمات الاتصال بالشبكة

ليتم الاتصال بالشبكة العالمية لابد من توافر عدة أشياء : -

١ - حاسب آلي

٢ - جهاز مودم

٣ - خط تليفون

٤ - الاشتراك في الخدمة

( في مصر و بعض الدول العربية اصبح الاشتراك في تلك الخدمة مجانا - فقط مقابل سداد مقابل الخدمة التليفونية )

٥ - وجود برامج تصفح شبكة الإنترنت ومن اشهرها

( INTERNET EXPLORER ) ( NETSCAPE )

## جرائم الإنترنت

### INTERNET CRIMES

تعتبر جرائم الإنترنت هي النوع الشائع الآن من الجرائم إذ أنها تتمتع بالكثير من المميزات للمجرمين تدفعهم إلى ارتكابها ويمكن تعريف تلك الجرائم بأنها (( الجرائم التي لا تعرف الحدود الجغرافية CRIMES TRANS BORDER و التي يتم ارتكابها بأداة هي الحاسب الآلي COMPUTER عن طريق شبكة الإنترنت و بواسطة شخص على دراية فائقة بها ))

## خصائص جرائم الإنترنت

### CHARACTERISTICS OF INTERNET CRIMES

و تعتبر الجرائم التي ترتكب من خلال شبكة الإنترنت INTERNET CRIMES هي جرائم ذات خصائص CHARACTERISTICS متفردة خاصة بها لا تتوافر في أي من الجرائم التقليدية في أسلوبها و طريقة ارتكابها و التي ترتكب يوميا في كافة دول العالم و التي لها خصائص أخرى مغايرة تماما لخصائص تلك الجرائم التي ترتكب عبر الإنترنت وتلك الخصائص الخاصة بجرائم الإنترنت هي :-

- ١ - في جميع الأحوال يكون الحاسب الآلي هو أداة ارتكاب الجريمة
- ٢ - ترتكب تلك الجرائم عبر شبكة الإنترنت
- ٣ - أن مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي
- ٤ - أن الجريمة لا حدود جغرافية لها

الخاصية الأولى : الحاسب الآلي هو أداة ارتكاب جرائم الإنترنت

**THE FIRST CHARACTERISTIC :  
THE COMPUTER IS THE COMMITTING  
UTENSIL OF THE INTERNET CRIMES**

خاصية أن الحاسب الآلي COMPUTER هو دائما أداة الجريمة في الجرائم التي ترتكب على شبكة الإنترنت هي خاصية متفردة عن أي جريمة أخرى ذلك أن الحاسب الآلي هو الأداة الوحيدة التي تمكن الشخص من الدخول على شبكة الإنترنت INTERNET و قيامه بتنفيذ جريمته أيا كان نوعها و عليه فالحاسب الآلي هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم التي ترتكب على شبكة الإنترنت .

الخاصية الثانية : الجرائم ترتكب عبر شبكة الإنترنت

**THE SECOND CHARACTERISTIC :  
CRIMES IS COMMITTING ACROSS THE  
INTERNET**

تعد شبكة الإنترنت INTERNET هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم AIMS OF CRIMES كالبنوك و الشركات الصناعية و غيرها من الأهداف التي ما تكون غالبا الضحية لتلك الجرائم و هو ما دعا معظم تلك الأهداف إلى اللجوء إلى نظم الأمن الإلكترونية ELECTRONIC SECURITY SYSTEMS في محاولة منها لتحمي نفسها من تلك الجرائم أو على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم .



الخاصية الثالثة : مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي

**THE THIRD CHARACTERISTIC :  
THE CRIMINAL IS A PERSON HAVING A  
LOT OF EXPERIENCE WITH COMPUTERS**

لاستخدام الحاسب الآلي COMPUTER لارتكاب جريمة على شبكة الإنترنت لابد و أن يكون مستخدم هذا الحاسب الآلي على دراية فائقة و ذو خبرة كبيرة في مجال استخدامه وإلا فأين له بالخبرة اللازمة التي تمكنه من تنفيذ جريمته و العمل على عدم اكتشافها ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي و أن الشرطة تبحث أول ما تبحث عن خبراء الكمبيوتر عند ارتكاب الجرائم

الخاصية الرابعة : الجريمة لا حدود جغرافية لها

**THE FOURTH CHARACTERISTIC :  
THE CRIME HAVE NO BORDER**

شبكة الإنترنت ألغت أي حدود جغرافية فيما بين الدول و بعضها إذ يمكن التحدث فيما بين أشخاص ليس في بلدان مختلفة و إنما في قارات مختلفة في نفس الوقت على شبكة الإنترنت من خلال الدردشة ( CHATING ) و عليه فإن أي جرائم ترتكب عبر شبكة الإنترنت INTERNET CRIMES فإنها تتخطى حدود الدولة التي ارتكبت فيها لتتعدى آثارها كافة البلدان على مستوى العالم .

## أهداف الجرائم الإلكترونية

### AIMS OF ELECTRONIC CRIMES

ومن المعروف أن أكثر الجرائم الإلكترونية التي يتم ارتكابها يكون الهدف الأساسي لها هو الحصول على المعلومات الإلكترونية التي تكون اما محفوظة على أجهزة الحاسبات الآلية أو تلك المنقولة عبر شبكة الإنترنت الا ان ذلك لا يعنى أن هناك جرائم أخرى يكون لها هدف آخر غير الحصول على المعلومات مهما كانت أهمية تلك المعلومات و عليه فسوف نعرض لأهداف الجرائم الإلكترونية .

### INFORMATION

#### ١ - المعلومات

هناك العديد من الجرائم التي يكون ارتكابها لهدف يتعلق بالمعلومات و يتمثل هذا الهدف أما بالحصول على المعلومات أو تغييرها أو حذفها فهائيا و هذا الهدف تعرضنا له تحت عنوان أمن المعلومات .

و معظم تلك الجرائم التي يكون الهدف منها المعلومات هي في الأغلب الأعم من الحالات تكون جرائم اقتصادية للحصول على مزايا أو مكاسب اقتصادية فالحرب الاقتصادية لا تقل في ضراوتها و شدتها حاليا عن الحرب العسكرية إلا انه تتم عبر شبكة الإنترنت .

#### ٢ - أجهزة الكمبيوتر

أما عندما يكون الهدف من ارتكاب الجرائم الإلكترونية عبر شبكة الإنترنت هو أجهزة الكمبيوتر فالغالب يكون الهدف هو تخريب تلك الأجهزة نهائيا او على

الأقل تعطيلها لأطول فترة ممكنة و معظم تلك الجرائم تتم بواسطة استخدام الفيروسات .

### ٣ - الأشخاص أو الجهات

معظم الجرائم التي ترتكب عبر شبكة الإنترنت تستهدف اما اشخاص أو جهات بعينها و غالبا ما تكون تلك الجرائم هي جرائم مباشرة ترتكب في صورة ابتزاز أو التهديد أو التشهير أو هي جرائم غير مباشرة ترتكب في صورة الحصول على البيانات و المعلومات الخاصة بتلك الجهات أو الأشخاص و ذلك لاستخدم تلك المعلومات و البيانات بعد ذلك في ارتكاب جرائم مباشرة .

### أضرار جرائم الإنترنت

## DAMAGES OF INTERNET CRIMES

وقد أجريت عدة دراسات عن جرائم الإنترنت INTERNET CRIMES منها تلك الدراسة التي أجرتها منظمة ( BUSINESS SOFTWARE ALLIANCE ) في الشرق الأوسط والتي أظهرت أن هناك تباين بين دول الشرق الأوسط في حجم خسائر DAMAGES جرائم الإنترنت و جرائم الحاسب الآلي حيث تراوحت بين ثلاثين مليون دولار أمريكي في المملكة العربية السعودية و الإمارات العربية المتحدة و مليون و أربعمائة ألف دولار أمريكي فقد في لبنان .

وقد أظهرت دراسة أخرى أجرتها هيئة الأمم المتحدة حول جرائم الإنترنت أيضا حوالي أربعون في المائة من منظمات القطاع العام و الخاص على السواء كانت ضحية لجرائم الإنترنت INTERNET CRIMES والحاسب الآلي .

وقد قدرت الولايات المتحدة الأمريكية اضرار جرائم الإنترنت DAMAGES OF INTERNET CRIMES و الحاسب الآلي التي تكبدتها حوالي خمسة مليارات دولار سنويا كما قدرت المباحث الفيدرالية الأمريكية ( F.B.I ) أن تكلفة جريمة الحاسب الآلي أو الإنترنت الواحدة حوالي ستمائة ألف دولار سنويا مقابل مبلغ ستة آلاف دولار تكلفة من جرائم السرقة بالإكراه و بينت دراسة أخرى أجراها أحد مكاتب المحاسبة الأمريكية أن حوالي مائتين و أربعون شركة أمريكية قد تضررت من جرائم الغش باستخدام الكمبيوتر ( COMPUTER FRAUD ) و أظهرت دراسة أخرى أجريت من قبل منظمة ( THE COMPUTER SECURITY INSTITUTE ) عام ١٩٩٩ م أن خسائر حوالة مائة و ثلاثة و ستون شركة أمريكية من جرائم الحاسب الآلي و الإنترنت قد بلغت أكثر من مائة و ثلاثة و عشرون مليون دولار في حين أن الدراسة التي أجريت في عام ٢٠٠٠ م قد أظهرت أن عدد الشركات التي تضررت قد زاد إلى أن أصبح مائتان و ثلاثة و سبعون شركة تخطت خسائرها مبلغ مائتان و ستة و خمسون مليون دولار .

ومثال ذلك ما أعلنته شبكة أخبار ( CNN ) تحت عنوان طالب يسطو على المعهد الذي يدرس به جاء فيه أن سلطات ولاية تكساس تحقق مع طالب يدعى ( فيليب اوستن ) قد سطا إلكترونيا على المعهد الذي يدرس به حيث استخدم كومبيوتر في اقتحام أنظمة الكومبيوتر الخاصة بالمعهد حيث سرق بيانات خاصة بالضمان الاجتماعي و كذلك بيانات شخصيه و معلومات خاصة عن حوالي خمسة و خمسون ألف طالب و عضو بهيئة التدريس بالمعهد و قد قرر الطالب انه لم تكن لديه أي نوايا إجرامية و انه لم يكن يخطط لاستخدام تلك البيانات في أي أنشطة إجرامية .

وعلى ذلك فنتيجة الإحصائيات التي أجرتها الجمعية الأمريكية للأمن الصناعي



طبيعية عندما أعلنت أن الخسائر DAMAGES التي تسببها جرائم الحاسب الآلي و جرائم الإنترنت INTERNET CRIMES للصناعات الأمريكية قد تصل إلى حوالي ثلاث و ستون مليار دولار وان حوالي ٢٥ % من الشركات الأمريكية تتضرر من تلك الجرائم .

### إثبات جرائم الإنترنت

و جرائم الإنترنت كثيرة و متنوعة و يصعب كشفها و حصرها و متابعة مرتكبها لان تلك الجرائم لا تترك أثرا يقود إلى مرتكبها مثل الجرائم التقليدية التي دائما ما تترك أثرا يقود إلى مرتكبها .  
و تعود أسباب صعوبة إثبات جرائم الحاسب الآلي و الإنترنت إلى خمسة أمور هم كالآتي :

- ١ - لا اثر للجريمة بعد ارتكابها
- ٢ - صعوبة الاحتفاظ الفني بآثارها أن وجدت .
- ٣ - أنها تحتاج إلى خبرة فنية و تقنية و يصعب على المحقق التقليدي التعامل معها .
- ٤ - أنها تعتمد على الخداع في ارتكابها و التضليل في التعرف على مرتكبها .
- ٥ - أنها تعتمد على قمة الذكاء و المهارة في ارتكابها .

ومع كل تلك المصاعب إلى تواجه إثبات جرائم الحاسب الآلي و الإنترنت PROVING THE INTERNET CRIMES ألا أن الأمر ليس بكل تلك الصعوبة ألا انه لا بد من الأخذ بعدة خطوات ليكون في الإمكان مكافحة

مثل تلك النوعية من الجرائم و تلك الخطوات هي : -

- ١ - تحديد الجريمة من البداية .
- ٢ - تحديد الجهة التي المنوط بها التعامل مع تلك الجرائم .
- ٣ - العمل على تأهيل عناصر تلك الجهات يكونوا على المستوى التقني الذي يمكنهم من العمل و مواجهة هذا النوع من الجرائم .
- ٤ - تعديل القوانين بما يتناسب مع تلك الجرائم التي استجدت على و وضع العقاب الشديد لها لتكون مانعا من موانع ارتكاب مثل تلك الجرائم .
- ٥ - التركيز على مواجهة تلك الجرائم **CRIMES** بصفة دولية بإقرار اتفاقات دولية تجرم تلك الجرائم و تعمل كل الدول على ملاحقة مرتكبيها .

### فوائد شبكة الإنترنت للأمن

هذا من جهة و من جهة فأن شبكة الإنترنت **INTERNET** ليست فقط مرتعا لارتكاب الجرائم و إنما هي أيضا تقدم خدمات جليلة للأمن بصفة خاصة نوجزها كالآتي : -

- ١ - تلقى البلاغات بطريقة فورية و سريعة .
- ٢ - إضفاء نطاق من السرية فيما بين الأمن و المتعاونين معهم بمعنى عدم تعريض المتعاونين مع الأمن للخطر .
- ٣ - إعطاء الفرصة لمن لديه معلومات من الجمهور أن يقدمها للأمن بطريقة سرية دون تعريض أمنه للخطر .

- ٤ - يمكن الأمن من توسيع إطار البحث عن المجرمين بنشر صورهم وطلب الإبلاغ عن أي معلومات عنهم على الشبكة ليطلع عليها أكبر عدد ممكن من الأشخاص لتضييق الخناق عليهم و يتم القبض عليهم .
- ٥ - وسيلة لنشر أي معلومات أو بيانات أو قوانين أو قرارات جديدة تهم المواطنين .
- ٦ - في بعض البلاد يتم تكوين جمعيات أهلية - غير حكومية - مهمتها مساعدة الشرطة في مهام عملها و التواصل بين تلك الجمعيات و الشرطة عن طريق شبكة الإنترنت INTERNET يسهل من عملية التواصل بينهم و يفعل تلك المساعدة المقدمة من تلك الجمعيات إلى الشرطة .
- ٧ - إذا ما اصدر الأمن أي نشرات تتضمن توعية أو تعليمات للجمهور فإن نشر تلك النشرات على شبكة الإنترنت هي الطريقة المثلى لتوعية الجمهور بتلك النشرات وما تحتويه من تعليمات على المواطنين أن يلتزموا بها .
- ٨ - من خلال شبكة الإنترنت و ما عليها من مواقع تهتم بتوفير فرص العمل للشباب يمكن العمل على حل واحدة من أهم المشكلات التي تعترض عمليات التنمية في البلاد ألا وهي البطالة .
- ٩ - يتم استخدام المواقع على شبكة الإنترنت في عمل الاستفتاءات على جميع القضايا سواء الوطنية أو العالمية و من خلال تلك الاستفتاءات يتم قياس مستوى رأى الجمهور فيما يعرض على القيادة السياسية من قضايا وطنية .
- ١٠ - تعتبر شبكة الإنترنت INTERNET بما تمثله من تقدم تقني

- **MODERN TECHNIQUES** من أهم أدوات التواصل فيما بين الشعوب و بعضها البعض و بالتالي يمكن استغلال هذا التواصل في نقل التقدم التكنولوجي و العلمي بمعظم أنواعه من الدول المتقدمة إلى الدول النامية و العمل على نقل التقدم الثقافي **MODERN CULTURAL** و العلمي أيضا و بالتالي تعتبر هذه الشبكة من أهم الطرق لرفع المستوى العلمي و التكنولوجي و الثقافي أيضا للشعوب النامية دون أن تكلفها أي من الأموال الطائلة التي كانت ستدفعها فيما لو طالبت تلك الدول المتقدمة مباشرة بهذه التكنولوجيات الجديدة و التي يمكنها الحصول عليها عبر شبكة الإنترنت و بدون أي مقابل مادي كما يمكنها أيضا من تدريب طلابها و علمائها عبر البرامج الدراسية الكثيرة و المتخصصة عبر الإنترنت دون أن تتكلف مبالغ كثيرة .

- ١١ - تعتبر الشبكة وسيطا فاعلا في عملية تدريب العاملين بمختلف المصانع و الشركات و تعريفهم بأحدث أساليب العمل في المصانع و الشركات المشابهة في الدول المتقدمة .

## طرق ارتكاب جرائم الحاسب الآلي و الإنترنت EXECUTION WAYS OF THE INTERNET CRIMES

ينمكن تقسم تلك الجرائم التي ترتكب عبر شبكة الإنترنت إلى أنواع بحسب ما تستهدفه من الجريمة و الطريقة في بلوغ هذا الهدف و على ذلك يمكن تقسيمها إلى أربع أنواع : -



## النوع الأول TYPE 1

وهي الجرائم التي تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي ( COMPUTER ) لاستغلالها بطريقة غير مشروعة و يتميز هذا النوع من الجرائم بصعوبة اكتشافه .

## النوع الثاني TYPE 2

وهذا النوع من الجرائم يستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بما أو تدميرها كلياً أو جزئياً و يمثل هذا النوع الفيروسات المرسلة عبر البريد الإلكتروني ( E - MAIL ) أو بواسطة برنامج ( PROGRAM ) مسجل في أحد الوسائط المتنوعة و الخاصة بتسجيل برامج الحاسب الآلي COMPUTER و يمكن اكتشاف هذا النوع من الفيروسات في معظم الحالات وذلك بواسطة برامج حماية متخصصة للبحث عن هذه الفيروسات و لكن يشترط الأمر تحديث قاعدة بيانات DATA BASE برامج الحماية لضمان أقصى درجة من الحماية .

مع الوضع في الاعتبار أن وجود مثل هذه البرامج في جهاز الحاسب الآلي لا يعنى إطلاقاً الحماية التامة من أي هجوم فيروسي وان ما من سبيل للوقاية إذا ما كان الهجوم بفيروس حديث لم يتم اكتشافه بعد ولم يتم تجهيز برامج للحماية منه بعد .

## النوع الثالث TYPE 3

و هو استخدام الحاسب الآلي ( COMPUTER ) في ارتكاب الجريمة وقد وقعت جريمة من هذا النوع في إحدى الشركات الأمريكية التي تعمل سحباً على جوائز يانصيب حيث قام أحد الموظفين بالشركة بتوجيه الحاسب الآلي

لتحديد رقم معين كان قد اختاره هو فذهبت الجائزة لشخص بطريقة غير مشروعة .

## النوع الرابع TYPE 4

و تشمل إساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل الأشخاص المرخص لهم باستخدامه و مثال ذلك استخدام الموظف الحاسب الآلي في أمور خاصة لا تختص بالعمل بعد انتهاء وقت العمل .

## الفصل الثاني



## أنواع الجرائم التي ترتكب عبر شبكة الإنترنت TYPES OF INTERNET CRIMES

نستعرض الآن الجرائم التي ترتكب على شبكة الإنترنت ماهيتها و وصفها القانوني و وسائل مكافحتها وهي كالآتي :

### ١ - الجرائم و الممارسات الجنسية و غير الأخلاقية

- المواقع الإباحية
- مواقع قذف و تشويه سمعة الأشخاص
- الدخول إلى المواقع المحجوبة
- إخفاء الشخصية
- انتحال الشخصية
  - انتحال شخصية الفرد
  - إنتحال شخصية المواقع

### ٢ - جرائم الاختراق

- الاقتحام أو التسلل
- الإغراق بالرسائل
- فيروسات الحاسب الآلية
  - خطورة برنامج حصان طروادة
  - أهم المنافذ المستخدمة لاختراق الجهاز

### ٣ - الجرائم المالية

- جرائم السطو على أرقام البطاقات الائتمانية
- القمار عبر الإنترنت
- تزوير البيانات



- الجرائم المنظمة
- تجارة المخدرات عبر الإنترنت
- غسل الأموال

- ٤ - المواقع المعادية
- ٥ - جرائم القرصنة
- ٦ - التجسس الإلكتروني
- ٧ - الإرهاب الإلكتروني

أولا : الجرائم و الممارسات الجنسية و غير الأخلاقية

## ١ - المواقع الإباحية

### UNIHIBITED LOCATIONS

لقد وفّرت شبكة الإنترنت أكثر الوسائل فعالية و جاذبية لصناعة و نشر الإباحية الجنسية فأن شبكة الإنترنت جطت الإباحية بشتى وسائل عرضها من صور و فيديو و حوارات سواء كانت مسجلة أو مباشرة في متناول الجميع و يعتبر ذلك من أكبر سلبيات شبكة الإنترنت .

فأن التأثير على البلاد حاليا يكون من خلال التأثير على شبابها فهو الأساس الذي تركز عليه البلاد في تحقيق نموها و طموحاتها و تهدف إليه في مستقبلها و عليه و لما كانت شبكة الإنترنت INTERNET هي شبكة مفتوحة مليئة بما هو مفيد ألا أنها أيضا مليئة بكل ما هو محرم و مرفوض طبقا لديننا و طبقا لتقاليدنا الشرقية .

ولما كانت المواقع الجنسية الإباحية UNIHIBITED LOCATIONS الموجودة بكثرة على شبكة الإنترنت تريد تحقيق الكثير من المكاسب المادية عن طريق زيادة مرتاديهما فأنها تشترط دفع مبالغ مالية مقابل الحصول على خدماتها المتمثلة في عرض و تحميل الأفلام البورنو الإباحية فأنها تحاول ذلك عن طريق إعطاء مرتادي تلك المواقع العديد من الصور الجنسية بلا أي مقابل مادي لتحاول جذب من يرتاد تلك المواقع إليها .

وزيادة على ذلك فأن تلك المواقع الإباحية تحاول في كل وقت تسهيل عملية الدخول على مواقعها و كذلك تسهيل عملية الحصول على ما تقدمه من برامج و أفلام و صور إباحية لمرتاديهما .

وقد يبدو للبعض أن تلك المشكلة هي مشكلة محلية خاصة بنا في منطقة الشرط الأوسط على أساس أن عاداتنا و تقاليدنا ترفض ذلك و تحرمه ألا أن تلك المشكلة هي مشكلة عالمية تحاول كل الدول كل بطريقتها مقاومة تلك المشكلة والحد من آثارها .

ومثال ذلك التقرير الذي نشرته شبكة ( C N N ) الإخبارية بتاريخ ١٥ / ٣ / ٢٠٠٣ في موقعها على شبكة الإنترنت ( WWW.CNN.COM ) بعنوان - سهولة الوصول إلى الملفات الإباحية - ذكرت فيه أن الوصول الآن إلى الملفات الإباحية أصبح بنفس السهولة التي يمكن الوصول بها إلى ملفات الموسيقى ( M P 3 ) و أنه يمكن أيضا تحميل الملفات الإباحية بنفس السهولة عند تحميل ملفات الموسيقى ( M P 3 ) وان ذلك يتم بالرغم من كافة الإجراءات التكنولوجية التي تم اتخاذها للحد من ذلك .

وقد ذكرت الشبكة في تقريرها أن هذا الموضوع الهام منظور حاليا أمام لجنة إصلاح حكومية أمريكية بهدف معالجة تلك الظاهرة والحد منها .

أما القوائم البريدية فهي اسهل إنشاء و غالبا ما تكون مجانية و يقوم أعضائها من المشتركين بتبادل الصور و الأفلام الإباحية على عناوينهم البريدية و يشترك في القوائم البريدية آلاف الأشخاص التي تصل أي رسالة يرسلها مشترك منهم إلى جميع المشتركين مما يعنى كم هائل من الصور و الأفلام الإباحية يتبادلها مشتركى القوائم البريدية بشكل يومي .

و يوجد على الإنترنت حاليا آلاف المواقع الإباحية الجنسية و التي أصبحت أكثر تخصصية فمنها من هو متخصص في أفلام الفيديو و منها من هو متخصص في الصور و الكثير منها متخصص في برامج المحادثة ( CHATTING ) و للأسف فأن كل تلك الأنواع من المواقع تجد الكثير جدا من الإقبال على زيارتها و تصفح محتوياتها الإباحية .

وفى دراسة أجرتها شبكة ( B B C ) عام ١٩٩١ م أن معدل التدفق على زيارة تلك المواقع الإباحية في أوقات العمل و التي تبدأ من الساعة التاسعة صباحا و حتى الخامسة عصرا تمثل حوالي ٧٠ % من إجمالي نسبة التدفق على زيارة تلك المواقع .

و كشفت دراسة أخرى أجراها الدكتور / مشعل القدهي - بأن هناك إقبالا كبيرا على زيارة تلك المواقع الإباحية **UNIHIBITED LOCATIONS** حيث ذكرت شركة ( **PLAY BOY** ) الإباحية و التي تصدر مجلة إباحية بنفس الاسم بأن ٤,٧٠ مليون زائر يزورون صفحاتها على شبكة الإنترنت أسبوعيا وان هناك بعض الصفحات الإباحية المشابهة تستقبل أكثر من ربع مليون زائر يوميا كما وجد أن أكثر من ( ٨٠ % ) ثمانين في المائة من الصور المتداولة في المجموعات الإخبارية هي صور إباحية و أن أكثر من ٢٠ % عشرون بالمائة من سكان الولايات المتحدة الأمريكية يزورون تلك الصفحات الإباحية حيث تبدأ زيارة تلك المواقع **LOCATIONS** أولا بهدف الفضول و معرفة محتوياتها ثم يتطور الأمر فسيما بعد إلى الإدمان على زيارة تلك المواقع وهو ما تستغله تلك المواقع في وضع رسوم يجب سدادها أولا قبل السماح بالدخول إلى الموقع و مشاهدة و تحميل ما يحتويه من ملفات الأفلام و الصور الإباحية وهو ما يحقق لها أرباح خيالية .

ويؤكد ذلك ما نشر من أن مجموع مشتر و ات المواد الإباحية من شبكة الإنترنت في عام ١٩٩٩ م ما نسبته ٨ % من دخل التجارة الإلكترونية البالغ ١٨ مليار دولار أمريكي في حين بلغ مجموع الأموال المنفقة للدخول على المواقع الإباحية **UNIHIBITED LOCATIONS** ما قيمته ( ٩٧٠ ) مليون



دولار أمريكي و وصل المبلغ في عام ٢٠٠٣ م إلى حوالي ثلاثة مليار دولار أمريكي .

ومن جهة أخرى فقد أوضحت دراسات أجريت أن أكثر زوار المواقع الإباحية هم من الشباب التي تتراوح أعمارهم بين ( ١٢ ) و ( ١٥ ) عاما في حين تمثل الصفحات الإباحية أكثر صفحات الإنترنت طلبا .

كما أوضحت دراسة أجرتها ( ADSIT - 1999 ) أن المواقع الإباحية أضحت مشكلة حقيقية وإن آثارها تطول كافة المجتمعات دون أن تعوقها أي حدود جغرافية .

وقد جرى حصر المواقع الإباحية العربية ARABIC UNINHIBITED SITES فقط دون الأجنبية في بعض المواقع على شبكة الإنترنت و منها موقع ( YAHOO ) فوجد أنها تصل إلى ( ١٧١ ) موقع بلغ عدد أعضاء أقلها إلى ( ٣ ) في حين بلغ عدد أكثرها أعضاء إلى ( ٨٦٨٣ ) عضوا و العدد في ازدياد .

وأخيرا لابد من الربط بين زيارة مثل تلك المواقع الإباحية الخليعة و التي تضغط على الفرائز و تثيرها في مجتمعات محافظة جنسيا كالمجتمعات العربية و بين زيادة الجرائم الجنسية التي زاد عددها .

### التكليف القانوني للجريمة

الإباحية الجنسية هي أمر مجرم في كافة القوانين العربية بل و في الكثير من القوانين في معظم بلاد العالم و تدرج تحت جريمة مسماها : -  
( ( إتيان الأعمال الفاضحة علنية و التحريض على ممارستها ) )  
و يعد من الأمور المشددة في التجريم أمرين هما : -

- ١ - العلنية أثناء ممارسة هذا الفعل
  - ٢ - العلانية في التحريض على ممارسته
- و مثال ذلك ما هو منصوص عليه في قانون العقوبات المصري من تجريم لتلك الأفعال و عقاب من يقوم بها .
- إذ ينص قانون العقوبات المصري في مواده على معاقبة
- كل من وجد في الطريق العام أو مكان مطروق يحرض المارة على الفسق بإشارات أو أقوال .

المادة ٢٦٩ مكرر

- كل من فعل علانية فعلا فاضحا مخلا بالحياء .

المادة ٢٧٨

و لما كانت شبكة الإنترنت INTERNET تعد مكانا مطروقا من الكثير من الشخصيات بل أنها مطروقة من أشخاص من كافة الجنسيات على مستوى العالم وهو ما يجعلها تحمل نفس خصائص الطريق العام أو المكان المطروق المنصوص عليهما في قانون العقوبات المصري .

كما أن شبكة الإنترنت تحمل صفة العلنية بمعنى أن من يقوم بفعل على الشبكة يكون بإمكان أي من مرتادي الشبكة الاطلاع عليه .

و لما كانت المواقع الإباحية UNINHIBITED LOCATIONS المنتشرة على شبكة الإنترنت INTERNET هي مواقع تحرض على الفسق و الأكثر من ذلك أنها لا تحرض على الفسق فقط بالإشارة و القول و إنما أكثر من ذلك فهي تحرض على الفسق بالصور و أفلام البورنو - الجنس - وهو الفعل الذي تم النص عليه في المادة<sup>١</sup> ( ٢٦٩ ) من قانون العقوبات المصري .

بل أن المحادثات الجنسية التي تتم غالبا من خلال ما يعرف بغرف المحادثات

( CHATTING ) تدرج تحت فعل الأفعال الإباحية الفاضحة التي تتم علانية و التي تم النص على تجريمها طبقا للمادة ( ٢٧٨ ) من قانون العقوبات المصري .

هذا من جهة و من جهة أخرى فإن كافة القوانين العربية تتعرض لذات الموضوع و لا اختلاف بينها في ذلك فكافة القوانين العربية قد جرمت تلك الأفعال المخالفة لتعاليم كافة الأديان السماوية .

## ٢ - مواقع قذف و سب و تشويه سمعة الأشخاص

مع انتشار الشائعات و الأخبار الكاذبة والتي تطول و تمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية حتى أنها طالت الرموز الدينية أيضا ظهرت على شبكة الإنترنت بعض المواقع المشبوهة و التي جندت نفسها لهدف واحد هو خدمة تلك الشائعات و الأخبار الكاذبة و ذلك بهدف قذف و سب و تشويه سمعة تلك الرموز السياسية و الفكرية و حتى الدينية والتي تلتف حولها الشعوب و الهدف الأساسي من تلك المواقع هو كما ذكرنا هو تشويه تلك الرموز بهدف تشكيك الناس في مدى مصداقية هؤلاء الأفراد و محاولة فسخ الناس من حولهم ليخلوا لهم الجو في محاولة منهم لتسميم أفكار الناس .

هذا من جهة و من جهة أخرى فقد يكون الهدف من تلك المواقع محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم إذا لم يرضخوا و يدفعوا مقابل مادي لعدم التعرض لهم و تركهم دون تشويه سمعتهم .

و مثال ذلك ما حدث في بداية دخول الإنترنت جمهورية مصر العربية عندما فسخت فتاة خطبتها من شاب و لرغبتة في الانتقام منها لفسخ خطوبتها منه

صمم موقعا على شبكة الإنترنت INTERNET و خصصه لنشر الأكاذيب عن تلك الفتاة و عن فساد أخلاقياتها و دينها و الأكثر من ذلك أنه قام بنشر أرقام تليفوناتها و مكان عملها و بدأت الفتاة في تلقي مكالمات سيئة من أشخاص مجهولين طالعوا ذلك الموقع LOCATIONS و قاموا بالاتصال بها تأسيسا على المعلومات المنشورة في الموقع مما حدا بالفتاة إلى إبلاغ الشرطة التي قامت بتحرياتها التي أثبتت كذب تلك المعلومات التي نشرت بذلك الموقع و بدأت في تتبع ذلك الشخص الذي نشر تلك المعلومات على هذا الموقع إلى أن أثبتت التحريات أن مصمم ذلك الموقع هو خطيبها السابق بغرض الانتقام منها لفسخها خطبتها منه .

وعليه فهذا مثال على موقع صمم بهدف واحد هو سب و قذف و تشويه سمعة فتاة لا لهدف إلا لأنها فسخت خطبتها .

و مثال آخر عندما تمكن المباحث في جمهورية مصر العربية من ضبط مهندس كومبيوتر مصري بتهمة نشر معلومات كاذبة على الإنترنت للتشهير بعائلة مسئول مصري و عائلته و ابنته و تصميم موقع CREATE LOCATIONS على شبكة الإنترنت لهذا الغرض .

و أشارت الصحف إلى أن ابنة المسئول المصري كانت عرضة للتشهير بعد أن قام أحد الأشخاص بنشر موقع على شبكة الإنترنت باستخدام بيانات عن الضحية بغرض التشهير بها

و أن إدارة مكافحة جرائم الحاسبات و شبكات المعلومات بوزارة الداخلية المصرية قد تمكنت بالتنسيق مع المباحث العامة في ضبط الشخص الذي قام بالتشهير بابنة المسئول الكبير و البالغة من العمر ثمانية عشر عام و نشر معلومات كاذبة حولها بهدف الإساءة إلى سمعتها و سمعة عائلتها و تبين بعد التحريات و المتابعة الإلكترونية التي قامت بها أن إدارة مكافحة جرائم



الحاسبات و شبكات المعلومات بوزارة الداخلية - وهي إدارة جديدة تم إنشاؤها حديثًا بوزارة الداخلية المصرية لمواجهة تلك الجرائم الإلكترونية الجديدة على المجتمع المصري - للشخص الذي قام بإنشاء ذلك الموقع **CREATE SITE** المسيء أن المتهم هو مهندس كومبيوتر و مصمم برامج و انه أنشا الموقع و المعلومات الملفقة بغرض التشهير و قد ضبطت الأجهزة الأمنية الشخص و تحفظت على جهاز الكومبيوتر المستخدم لكونه دليلا ماديا على ارتكاب تلك الجريمة الإلكترونية .

كما أن هناك حادثة أخرى مشهورة جرى تداولها بين مستخدمة الإنترنت في بداية دخول الخدمة في منطقة الخليج حيث قام شخص في دولة خليجية بإنشاء موقع على شبكة الإنترنت **INTERNET** نشر فيه صور لفتاة و هي عارية مع صديقها و كان قد حصل على تلك الصور بعد التسلل إلى جهاز الحاسب الآلي الخاص بتلك الفتاة و نسخ منه تلك الصور و لما حاول ابتزازها جنسيا بتلك الصور و رفضت قام بإنشاء ذلك الموقع و نشر فيه تلك الصور مما أدى بالفتاة إلى أن تنتحر بعد ما سببه لها من فضيحة بين أهلها و ذويها .

كما وقعت حادثة تشهير أخرى من قبل تصدى له من اسموا أنفسهم (( الأمجاد هكرز )) حيث اصدروا بيان نشر على الإنترنت بواسطة البريد الإلكتروني ووصل للعديد من مستخدمي الإنترنت أوضحوا فيه قيام شخص بالتطاول في أحد المنتديات بالنسب و القذف على شيخ الإسلام (( ابن تيميه )) و غيره من رموز الفكر الإسلامي الذي يلتف حولهم المسلمون لمعرفة أمور دينهم و دنياهم و قد استطاع من اسموا أنفسهم (( الأمجاد هكرز )) اختراق البريد الإلكتروني لهذا الشخص الذي قام بالتطاول على رموز الإسلام و من ثم تم نشر صورده و كشف أسرارده في موقعهم على الإنترنت لتجربته على ما ارتكب في حق رموز الإسلام .

## التكليف القانوني للجريمة

تعد جريمة السب و القذف و التعرض للحياة الشخصية للأفراد بغرض التشهير و الخوض في أعراضهم من اكبر الجرائم التي تم تجريمها في كافة القوانين سواء في الدول العربية أو الدول الأجنبية يا كانت الطريقة أو الوسيلة التي تتم بها تلك الجريمة سواء كانت تتم بالطرق التقليدية أو بالطرق الحديثة التي تتم

باستخدام شبكة الإنترنت بواسطة إنشاء مواقع **CREATE LOCATIONS** خاصة بقذف و سب و التشهير سواء بشخص معين أو بدولة من الدول أو بدين من الأديان .

و أسباب ذلك التجريم تنطوي على أن الحرية و الديمقراطية التي تنعم بها الشعوب لا يجب أن تنطوي على الإخلال بها و تجريح الأشخاص في أعراضهم و مبادئهم و شرفهم و نسب أمور غير صحيحة لهم بغرض التشهير بهم و بمبادئهم و الخوض في أعراضهم و في حياتهم الخاصة التي هي ملك لهم و ا حدهم دون أن يكون لأي شخص آخر أن يخوض أو يتدخل فيها بأي شكل من الأشكال .

و يمكن حصر الأمور المجرمة قانونا في جرائم القذف و السب التي تقه بالطرق التقليدية في الآتي : -

- إسناد أمور لو كانت صحيحة لأوجبت عقاب من تم إسناد هذا الأمر إليه أو احتقاره عن أهله .

- أي سب بحيث يكون متضمنا خدشا للشرف أو الاعتبار

- التعرض لأثني على وجه يخدش حياتها

- التعرض لحرمة الحياة الخاصة

و يمكن حصر الأمور المشددة للعقاب إذا ما ارتكبت الجرائم سالفه الذكر في الآتي :-

- إذا ما كان من تم سبه و قذفه موظفا عاما
- إذا ما تمت واقعة القذف و السب بطريق النشر في إحدى الجرائد أو المطبوعات

- إذا ما تمت واقعة القذف و السب بطريق التليفون
- إذا ما كان القائم بتلك الجريمة من تعرف على تلك الأمور بمناسبة قيامه بعمله كالصيادلة و الأطباء و غيرهم

و عليه فإن جريمة القذف و السب و التشهير التي تتم بالطرق الحديثة التي تتم باستخدام شبكة الإنترنت بواسطة إنشاء مواقع يكون هدفها فقط قذف أو سب أو التشهير سواء بشخص معين أو بدولة من الدول أو بدين من الأديان تقع تحت طائلة نفس النصوص القانونية التي تجرم تلك الأفعال متى تمت بالطرق التقليدية .

وفي القانون المصري فقد تم تجريم تلك الأفعال و تم النص في قانون العقوبات المصري على تجريم تلك الأفعال في المواد من المادة ( ٣٠٢ ) و حتى المادة ( ٣١٠ ) ففي المادة ٣٠٢ من قانون العقوبات المصري تم النص على انه يعد قاذفا كل من اسند لغيره أمورا لو كانت صادقة لأوجبت عقاب من أسندت إليه بالعقوبات المقررة قانونا أو أوجبت احتقاره عند أهل وطنه و قد تم النص في المادة ٢٠٣ على العقوبة PUNISHMENT المقررة في حالة ارتكاب تلك الجريمة بالحبس مدة لا تتجاوز سنتين و بغرامة لا تقل عن عشرين جنيها و لا تزيد عن مائتي جنيه أو بإحدى هاتين العقوبتين فقط .

و يلاحظ هنا ضعف العقوبة PUNISHMENT المقررة على تلك الجريمة

**CRIME** و ذلك على اعتبار أن ارتكاب تلك الجريمة في البيئة الاجتماعية المصرية قليل للغاية و انه يعد من اندر الحوادث على الإطلاق حيث أن العادات و التقاليد المصرية و العربية بصفة عامة تعمل على الارتقاء بالنفس و عدم إهانة الأشخاص مهما كانت درجة الاختلاف في الرأي .

بل أن المادة ٣٠٥ من ذات القانون قد نصت على أن من اخبر بأمر كاذب مع سوء القصد فيستحق العقوبة ولو لم يحصل منه إشاعة . . . . .

أما المادة ٣٠٦ فقد نصت على أن كل سب لا يشتمل على إسناد واقعة ومعينه بل يتضمن بأي وجه من الوجوه خدشا للشرف أو الاعتبار يعاقب عليه بالحبس مدة لا تجاوز سنة و بغرامة لا تزيد على مائتي جنيه أو بإحدى هاتين العقوبتين .

### ٣ - الدخول إلى المواقع المحجوبة

بعض الدول تعمل على حجب المواقع **LOCATIONS** غير المناسبة و المتماشية مع تقاليدها الاجتماعية و مثال ذلك أن بعض الدول تعمل على حجب المواقع الجنسية الإباحية حتى لا يستطيع زائري شبكة الإنترنت الدخول إلى تلك المواقع و تلك الدول تعمل على حماية تقاليدها و عاداتها الاجتماعية مما يمكن أن يسببه الدخول على تلك المواقع الإباحية **UNINHIBITED LOCATIONS** ألا أن بعض الأشخاص يعملون على الدخول إلى تلك المواقع بالرغم من حجبها باستخدام بعض البرامج المتخصصة في الدخول إلى المواقع المحجوبة و هؤلاء الأشخاص بذلك يرتكبون جريمة ينص عليها قانون الدولة التي تعمل على حجب تلك المواقع .



وعليه فإن هؤلاء الأشخاص عندما يستخدمون بعض البرامج بغرض الدخول إلى تلك المواقع المحجوبة يعتبرون مرتكبي جريمة الدخول إلى تلك المواقع على أساس أن قوانين تلك الدول التي تحجب تلك المواقع تجرم الدخول إلى تلك المواقع .

و نحن نرى أن حجب تلك البرامج هو تصرف صحيح بالنسبة إلى الأطفال اقل من السن التي يمكن أن يؤثر فيهم تلك المواقع و يستطيعون الفرار من تأثيرها الذي قد يعتبر مميتا على المحافظة على تعاليم الدين و العادات و التقاليد الاجتماعية السائدة في تلك الدول .

### التكليف القانوني للجريمة

الكثير من البلاد لا يتم إدخال خدمة الإنترنت بها إلا بعد إجراء ما يسمى بفترة المواقع أي أن الدولة تقوم بحجب بعض المواقع التي تجد أنها غير مناسبة للدخول عليها سواء لأسباب دينية أو سياسية و عليه فهي تقوم بفترة المواقع و حجب ما ترى أنه غير مناسب بحيث لا يكون من الممكن الدخول إلى تلك المواقع و عليه فالدخول إلى تلك المواقع في تلك البلاد تعد جريمة يعاقب عليها القانون .

و الدخول إلى تلك المواقع المحجوبة لا يكون مستحيلا على من يريد الدخول إذ توجد البرامج المتخصصة في ذلك و التي تمنع عملية الحجب التي تقوم بها الدولة .

و نحن هنا في مصر لا توجد أي مواقع محجوبة فالدولة تنتهج سياسة ترك الإنترنت دون أي حجب و تعمل في نفس الوقت على زيادة التوعية الدينية و الثقافية لأفراد الشعب .

#### ٤ - إخفاء الشخصية

نظرا للتطور الهائل في مجال البرمجيات على مستوى العالم و الذي نشهده اليوم و الذي يزداد كل فترة قصيرة فقد ظهرت بعض البرامج المتخصصة **SPECIAL PROGRAMS** التي يمكن استخدامها في إخفاء هوية الشخص عند الدخول على شبكة الإنترنت **INTERNET** و لكن غالبا ما يتم استخدام برامج **PROGRAMS** إخفاء الشخصية تلك عند الدخول على برامج التحدث **CHATING PROGRAMS** حتى يتمكن الشخص من التحدث كما يريد و في المواضيع التي يريد ها دون إعلان شخصيته الحقيقية كي لا يتعرف عليه أحد و هو ما يمكنه من التحدث في برامج التحدث **CHATING PROGRAMS** دون التزام بقوانين **LAWS** وهو ما يخجل من الحديث فيه في حالة ما إذا لو عرفت شخصيته الحقيقية و كذلك عند إرسال البريد الإلكتروني **SENDING E MAIL** - حتى لا يعرف المرسل إليه هذا البريد الإلكتروني من هو المرسل مما يمكن المرسل من أن يرسل أي شئ وقبح أو مخالف للقوانين دون الخواف من أن ينال عقاب ما فعله .

ألا انه و مع تقدم البرامج المتخصصة **SPECIAL PROGRAMS** فقد أمكن التعرف على الشخص حتى ولو حاول أن يخفي شخصيته ألا أن ذلك يتطلب الكثير من الجهد و نتائجه ليست مضمونة مائة في المائة في الوصول إلى شخصية المتحدث على برنامج المحادثة ( **CHATING** ) أو مرسل البريد الإلكتروني .

وفي معظم الأحوال قد يمكن معرفة الرقم أو المكان الذي تمكن منه هذا الشخص من الدخول على الإنترنت منه دون معرفة بياناته الحقيقية التي أخفاها .

## التكليف القانوني للجريمة

لا يعد إخفاء الشخصية جريمة في قوانين جمهورية مصر العربية إلا إذا تم الاستفسار عنها و لم تتم الاجابة بصورة صحيحة فتعد إخفاء البيانات من الظهور على الإنترنت لا يعد جريمة إلا انه في بعض البلاد الأخرى يعد هذا الاجراء جريمة يعاقب عليها القانون

### ٥ - إنتحال شخصية الفرد

تبدأ عملية انتحال الشخصية عبر الإنترنت عندما يستغل اللصوص بيانات شخص ما على الشبكة الإلكترونية أسوأ استغلال ومن هذه البيانات العنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابه من أجل الحصول على بطاقات ائتمانية أو رخص قيادة و عليه يستطيع المجرمون من خلال هذه المعلومات أن يخفوا شخصياتهم الحقيقية ويتصرفون بحرية تحت اسم مستعار وتمكن أرقام الضمان الاجتماعي والبيانات الأخرى لصصوص انتحال الشخصيات من التقدم بطلبات لاستخراج بطاقات ائتمانية عبر الإنترنت غالبا من خلال هيئات لا تتخذ الإجراءات الأمنية الصارمة عبر الشبكة فإذا قام أحد لصوص انتحال الشخصية بصناعة تاريخ جديد له عن طريق تسديد فواتير شهرية بالبطاقة الائتمانية سوف يكون له الأحقية في طلب قروض لشراء سيارات وإيجار العقارات وتشير هيئات وشركات البطاقات الائتمانية من طرفها إلى أن نسبة انتحال الشخصية ضعيفة جدا مقارنة بمئات المليارات من الدولارات التي تنفق عبر

### البطاقات الائتمانية سنويا .

و جريمة انتحال الشخصية جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية القديمة ألا انه و مع انتشار شبكة الإنترنت فقد اخذ هذا النوع من الجرائم شكلا جديدا مستفيدا من التطور التكنولوجي الذي تمثله شبكة الإنترنت INTERNET وغالبا ما يكون انتحال شخصية الشخص على شبكة الإنترنت غالبا مه يكون بهدف أما تشويه سمعة هذا الشخص أو استخراج بطاقات ائتمانية أو الاستيلاء على بعض ممتلكاته أو كلها أن أمكن بحسب الشخص المراد انتحال شخصيته و موافقه سواء السياسية أو الدينية أو درجة ثراءه و ما إلى ذلك من أسباب يتم من اجلها انتحال شخصية هذا الشخص .

و انتحال شخصية الشخص يتطلب كما ذكرنا سلفا الحصول على الكثير من المعلومات المتعلقة به و للحصول على تلك المعلومات يلجأ المنتحل إلى الكثير من الطرق الملتوية لمخاطبة هذا الشخص و الحصول من خلاله على تلك المعلومات أو أن يحاول اللجوء إلى وسائل إحتيالية أخرى بحيث يمكنه من خلالها الحصول على تلك المعلومات .

و غالبا ما يتحصل المنتحل على تلك المعلومات التي يريدتها عن طريق استغلال عادة الطمع التي توجد دائما في الكثير من الأشخاص و غالبا ما يتم ذلك عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الإنترنت و التي تخاطب غالبا غريزة الطمع في الإنسان في أن تمنيه بالفوز مثلا بجائزة غالية الثمن أو كبيرة القيمة مقابل ثمن قليل لا يقارن بتلك الجائزة وغالبا ما يتم استغلال ذلك في الوصول إلى الشخص المبراد انتحال شخصيته بهدف الحصول منه على أي معلومات تكون لازمة للمنتحل ليتمكن من إتمام عملية الانتحال .

و عملية انتحال الشخصيات هي جريمة مؤثمة و مجرمة قانونا في الكثير من الدول طبقا للقوانين التقليدية دونما احتياج إلى تعديل تلك القوانين لتستوعب تلك الجريمة فانتحال الشخصية هي جريمة قديمة AN OLD CRIMES فقد أصبحت تتم بأسلوب متطور تكنولوجيا دون الأسلوب الذي كانت تتم به قديما هذا بالنسبة إلى الأسلوب أما الجريمة نفسها فهي مجرمة نظرا لما يكابده الشخص الذي تم انتحال شخصيته من أضرار أقلها الأضرار المعنوية بجانب الأضرار المادية حيث أن انتحال الشخصية لا يتم إلا لخداف و سب هذا الشخص أو تشويه سمعته أو للحصول على بعض أو كل ما يملكه .

### التكييف القانوني للجريمة

اختلاس الألقاب و الوظائف و الاتصاف بها دون حق هي جريمة مؤثمة و مجرمة في القانون المصري و في كافة القوانين العربية .  
إلا أن تلك الجريمة التي ترتكب عبر الإنترنت تكون غالبا مقترنة بجريمة أخرى أما سرقة بيانات أو عمليات نصب و احتيال أو الاستيلاء على أملاك الغير أو ما إلى ذلك من جرائم أخرى غالبا ما تكون مقترنة بجريمة انتحال الشخصية .  
و تلك الجرائم المقترنة هي جرائم مؤثمة و مجرمة قانونا أيضا إلا أنها تعد عاملا مشددا للعقاب في جريمة انتحال الشخصية إذا ما اقترنت بها .  
و قد نص قانون العقوبات المصري على تلك الجرائم في المواد من ١٥٥ - ١٥٩ إلا أنه يؤخذ على المشرع المصري ضعف العقوبة المقررة على تلك الجرائم رغم أهميتها و ما يترتب عليها من أضرار هامة سواء مادية أو أضرار معنوية للشخص التي تمت انتحال شخصيته .



و نحن نرى أن المشرع المصري عليه أن يشدد كثيرا في العقاب المقرر على تلك الجرائم لما يترتب عليها من أضرار مادية و معنوية كبيرة تؤثر اشد التأثير على الشخص الذي تم انتحال شخصيته .

## ٦ - إنتحال شخصية المواقع

و إنتحال شخصية المواقع تعنى انه يمكن لبعض الأشخاص الدخول على الموقع و إما أن يحجبه و يضع الموقع الخاص به بدلا منه أو أن يغير هذا الموقع كما يحلو له ويحدث هذا في غالب الأحيان في المواقع السياسية أو الدينية وذلك لاسباب دينية أو سياسية .

ففي المواقع السياسية نرى هذا يحدث فيما بين المواقع الفلسطينية PALESTINIAN SITES و المواقع الإسرائيلية فكثيرا ما يدخل الفلسطينيون على المواقع الإسرائيلية و يقوموا بإلغاء الصفحة الرئيسية و يضعون بدلا منها العلم الفلسطيني و العكس بالعكس نرى انه يحدث أيضا أن يدخل بعض اليهود الإسرائيليين إلى بعض المواقع الفلسطينية PALESTINIAN SITES و يحاولون إلغاء الموقع و وضع بدلا منه صورة العلم الإسرائيلي و النشيد الوطني الإسرائيلي .

و انتحال المواقع هذا لا يحدث بين الإسرائيليين و الفلسطينيين فقد و إنما يحدث فيما بين كل طرفين بينهما أي مشكلة سياسية أو دينية فليست الحروب الحديثة كلها تدور الآن بالدبابات و الطائرات و إنما الكثير منها الآن يدور على أجهزة الكمبيوتر و على شبكة الإنترنت فسلح الكمبيوتر أصبح الآن من أهم الأسلحة التي تستخدم في المعارك نظرا لتأثيرها البالغ الأهمية على المعركة الإعلامية التي يدور رحاها بجانب المعارك العسكرية .

## التكليف القانوني للجريمة

نظرا لعدم وجود قوانين حتى الآن في مصر خاصة بالجرائم الإلكترونية فتطبق القوانين العادية الخاصة بالجرائم القديمة التقليدية على تلك الجرائم الإلكترونية الحديثة و عليه فيمكن القول انه تطبق القواعد القانونية الخاصة بانتحال الشخصية على تلك الجرائم المتعلقة بانتحال شخصية المواقع على أساس أن تلك المواقع لها شخصية معنوية تتساوى مع الشخصية الطبيعية التي يملكها الشخص العادي .

و عليه فالقواعد القانونية التي تطبق على جريمة انتحال شخصية الشخص العادة تطبق كما هي على جريمة انتحال شخصية المواقع .

## ثانيا : جرائم الاختراق

يعتبر الهجوم على المواقع و اختراقها على شبكة الإنترنت من الجرائم الشائعة في العالم

وطبقا لمؤشر سام للاختراق فإن لمستويات الاختراق او الهجوم المعلوماتي ستة مستويات بحسب درجة الخطورة : -

### - المستوى الأول من الهجوم ATTACK - LEVEL . 1

ما يعرف بهجوم قنبلة صندوق البريد وتؤدي إلي إعاقة النظام عن تقديم الخدمة .

### - المستوى الثاني من الهجوم ATTACK - LEVEL . 2

الدخول غير المرخص به لنظام المعلومات أو الحاسبات بما يتيح قراءة الملفات أو نسخها للمخترق غير المرخص له .

- المستوى الثالث من الهجوم ATTACK - LEVEL . 3

يمكن المخترق فيه من الدخول إلى مواقع غير مرخص في الدخول إليها .

- المستوى الرابع من الهجوم ATTACK - LEVEL . 4

يمكن المخترق فيه من قراءة ملفات سرية .

- المستوى الخامس من الهجوم ATTACK - LEVEL . 5

يمكن المخترق فيه من نقل ونسخ الملفات السرية .

- المستوى السادس من الهجوم ATTACK - LEVEL . 6

حيث يستطيع المخترق من خلال هذا المستوى من الاختراق أن يوجد قناة مفتوحة للدخول إلى سائر أرجاء النظام والعبث بمحتوياته .

هذا ويستخدم المهاجم في هجومه ما يعرف بالقتيلة المنطقية وهي برنامج يدمر البيانات أو قد يستخدم حصان طروادة وهو برنامج لاقتحام أمن النظام يتنكر في شكل برئ حتى يلج إلى النظام فيفسده .

## ١ - الاختراق

لكي تتم عملية الاختراق لابد من برنامج يتم تصميمه ليتيح للمخترق الذي يريد اختراق الحاسب الآلي لشخص آخر أن يتم ذلك الاختراق وقد صمم العديد من تلك البرامج التي تتيح عملية الاختراق و تجعلها سهلة ألا أن معظم تلك البرامج كان بها نقطة ضعف أساسية تقلل كثيرا من إمكانياتها و هي إمكانية الشعور بتلك البرامج على الجهاز الذي تم اختراقه و عليه يكون من الممكن متابعة تلك البرامج و القضاء عليها فيما عدا برنامج واحد تمكن مصمموه من التغلب على هذا العيب الموجود في كافة برامج الاختراق الأخرى

و أطلق على هذا البرنامج أسم ( حصان طروادة )  
و يعتبر برنامج حصان طروادة من البرامج الخطرة DANGEROUS  
PROGRAMS على الإطلاق التي تستخدم في عمليات اختراق أجهزة  
الحاسبات الآلية COMPUTERS نظرا لامتعه بعدة مميزات تجعل منه الأقدر  
على عملية الاختراق دون القدرة على كشفه و تتبعه و القضاء عليه لذلك  
فقد اكتسب هذا البرنامج شهرة كبيرة في مجال اختراق أجهزة الحاسبات  
الآلية .

صمم برنامج حصان طروادة في البداية بغرض حسن و مفيد هو معرفة ما  
يقوم به الأبناء على جهاز الكمبيوتر COMPUTERS في غياب الوالدين  
أو معرفة ما يقوم به الموظفون على جهاز الكمبيوتر في غياب المدراء ألا  
انه تم تطوير هذا البرنامج بعد ذلك تطورا سينا .

و تكمن خطورة هذا البرنامج ( حصان طروادة ) في كونه يتيح للمخترق أن  
يحصل على كلمة سر ( PASSWORDS ) الدخول على الجهاز بمعنى أنه  
يتيح للدخيل أن يتمكن من الدخول على الجهاز بطريقة لا تثير أي ريبة أو شك  
نظرا لأنه يمكن للدخيل من الدخول على جهاز الكمبيوتر COMPUTERS  
باستخدام كلمة السر ( PASSWORDS ) التي يستخدمها صاحب الجهاز و  
من هنا تكمن خطورة هذا البرنامج لان الدخول على الجهاز باستخدام كلمة السر  
لا يمكن صاحب الجهاز من ملاحظة وجود دخيل يتمكن من الدخول على الجهاز  
في غيبته .

ومن جهة أخرى فإن هذا البرنامج لا يمكن كشفه بواسطة البرامج المتخصصة  
في كشف الفيروسات و عليه فانه لا يمكن في الأغلب الأعم من الأحوال معرفة  
وجود مثل هذا البرنامج على جهاز الكمبيوتر أو الإحساس بوجوده للقضاء  
عليه ( NANOART - 2000 ) .

## كيفية اقتحام الجهاز

- لنتم عملية التسلل لابد من زرع حصان طروادة و يتم زرعه بعدة طرق :
- ١ - يرسل عن طريق البريد الإلكتروني ( E - MAIL ) كملف ملحق حيث يقوم الشخص باستقباله و تشغيله و قد لا يرسل لوحده حيث من الممكن أن يكون ضمن برامج أو ملفات أخرى .
  - ٢ - عند استخدام برنامج المحادثة الشهير ( I C Q ) و هو برنامج محادثة أنتجته إسرائيل
  - ٣ - عند تحميل برنامج من أحد المواقع غير الموثوق بها
  - ٤ - مجرد كتابة كوده على الجهاز نفسه
  - ٥ - في حالة اتصال الجهاز بشبكة داخلية أو شبكة إنترنت
  - ٦ - يمكن نقل البرنامج أيضا بواسطة استخدام برنامج ( F T P ) أو برنامج ( TELNET )
  - ٧ - كما يمكن الإصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكرو الموجود في برامج معالجة النصوص
- ومن ناحية أخرى فلنستطيع أي برنامج اختراق أن يتم عملية الاختراق نفسها لابد من وجود منافذ في الجهاز المراد اختراقه و من أهم تلك المنافذ التي يمكن استخدامها من قبل المتسللين و البرامج المستخدمة في النفاذ من هذه المنافذ :

2023	RIPPER
2115	BUGS
2140	DEEP THROAT . THE INVESOR



<b>2565</b>	<b>STRIKER</b>
<b>2583</b>	<b>WIN CRASH</b>
<b>2801</b>	<b>PHINEAS PHUCKER</b>
<b>3024</b>	<b>WIN CRASH</b>
<b>3129</b>	<b>MASTER PARADISE</b>
<b>3150</b>	<b>DEEP THROAT . THE INVASOR</b>
<b>3700</b>	<b>PORTAL OF DOOM</b>
<b>4092</b>	<b>WIN CRASH</b>
<b>4567</b>	<b>FILE NAIL</b>
<b>4590</b>	<b>ICQ TROJAN</b>
<b>5000</b>	<b>BUBBEL . BACK DOOR SETUP . SOCKETS DE TROIE</b>
<b>5001</b>	<b>BACK DOOR SETUP . SOCKETS DE TROIE</b>
<b>5321</b>	<b>FIRE HOTCKER</b>
<b>5400</b>	<b>BLADE RUNNER</b>
<b>5401</b>	
<b>5402</b>	
<b>5555</b>	<b>SERVE ME</b>
<b>5556</b>	<b>BO FACIL</b>
<b>5557</b>	
<b>5569</b>	<b>ROBO - HACK</b>
<b>5742</b>	<b>WIN CRASH</b>
<b>6400</b>	<b>THE THING</b>
<b>6670</b>	<b>DEEP THROAT</b>
<b>6711</b>	<b>SUB SEVEN</b>
<b>6771</b>	<b>DEEP THROAT</b>
<b>6776</b>	<b>BACK DOOR - G . SUB SEVEN</b>
<b>6939</b>	<b>INDOCTRINATION</b>
<b>6969</b>	<b>GATE CRASHER . PRIORITY</b>

<b>7300</b>	<b>NET MONITOR</b>
<b>7301</b>	
<b>7306</b>	
<b>7307</b>	
<b>7308</b>	
<b>7000</b>	<b>REMOTE GRAB</b>
<b>7789</b>	<b>BACK DOOR SETUP . ICKILLER</b>
<b>9872</b>	<b>PORTAL OF DOOM</b>
<b>9873</b>	
<b>9874</b>	
<b>9875</b>	
<b>10067</b>	
<b>10167</b>	
<b>9989</b>	<b>INI - KILLER</b>
<b>10520</b>	<b>ACID SHIVERS</b>
<b>10607</b>	<b>COMA</b>
<b>11000</b>	<b>SENNA SPY</b>
<b>11223</b>	<b>PROGENIC TROJAN</b>
<b>12223</b>	<b>HACK 99 KEY LOGGER</b>
<b>12345</b>	<b>GABAN BUS NET BUS PIE BILL GARES . X - BILL</b>
<b>12346</b>	<b>GABAN BUS NET BUS . X - BILL</b>
<b>12361</b>	<b>WHACK - A - MOLE</b>
<b>12363</b>	
<b>12631</b>	<b>WHCK JOP</b>
<b>13000</b>	<b>SENNA SPY</b>
<b>16969</b>	<b>PRIORITY</b>
<b>20001</b>	<b>MILLENNIUM</b>
<b>20034</b>	<b>NET BUS 2 PRO</b>
<b>21544</b>	<b>GIRL FRIEND</b>
<b>22222</b>	<b>PROSIK</b>

23456	EVIL FTP . UGLY FTP
26274	UPT - DELTA SOURCE
29891	UPT - THE UNEXPLAINED
30029	AOL TROJAN
30100	NET SPHERE
30101	
30102	
30303	SOCKETS DE TROIE
31337	BAROON NIGHT . BO CLIENT . BO 2 . BO FACIL UPD - BACK FIRE . BACK ORIFICE . DEPP BO
31338	NET SPY DK
31339	
31338	UPD - BACK ORIFIC . DEEP BO
31666	BO WHACK
33333	PROSIK
34324	BIG GLUCK . TN
40412	THE SPY
40421	AGENT 40421 . MASTER PARADISE
40422	MASTER PARADISE
40423	
40426	
47262	UPD - DELTA SOURCE
50505	SOCKETS DE TROIE
50766	FORE
53001	REMOTE WINDOWS SHUTDOWN
54321	SCHOOL BUS
60000	DEEP THROAT
61466	TELECOMMANDO
65000	DEVIL

المصدر : موقع

[HTTP://WWW.NANOART.F2S.COM/HACK/PORTS3.HTM](http://www.nanoart.f2s.com/hack/ports3.htm)

و المنافذ تلك يمكن وصفها ببوابات الجهاز و هناك ما يقرب من ٦٥٠٠٠ ( خمسة و ستون ألف ) منفذ تقريبا في كل جهاز و يميز كل منفذ عن الآخر برقم خاص به و لكل منفذ غرض محدد فمثلا المنفذ رقم ٨٠٨٠ يخصص أحيانا لمزود الخدمة و هذه المنافذ غير مادية مثل منفذ الطابعة و تعتبر جزء من الذاكرة لها عنوان معين يتعرف عليها الجهاز أحيانا بأنها منطقة إرسال و استقبال البيانات و كل ما يقوم به المتسلل هو فتح أحد هذه المنافذ للوصول إلى جهاز الضحية وهو ما يعرف بطريقة الزبون / الخادم ( CLIENT / SERVER ) حيث يتم إرسال ملف لجهاز الضحية ليقوم يفتح تلك المنافذ فيصبح جهاز الضحية ( SERVER ) و جهاز المتسلل ( CLIENT ) و من ثم يقوم المتسلل بالوصول إلى تلك المنافذ باستخدام برامج كثيرة متخصصة كبرنامج ( NET BUS ) أو ( NET SPHERE ) و لعل الخطوة الإضافية تكمن في انه عند دخول المتسلل إلى جهاز الضحية فانه لن يكون الشخص الوحيد الذي يستطيع الدخول إلى ذلك الجهاز حيث يصبح ذلك الجهاز مركزا عاما يمكن لأي شخص الدخول عليه بمجرد قيامه بعمل مسح للمنافذ ( PORTSCANNING ) عن طريق أحد البرامج المتخصصة في ذلك .

وقد كثرت حالات الاختراق عبر شبكة الإنترنت و كونها لم تعد تقتصر على المحترفين فقط بل أصبحت عمليات الاختراق يقوم بها بعض الهواة و تكون في قوتها وكأن محترفين شديدي الاحتراف هم القائمين بها .

فقد تعرضت مثلا مواقع وزارت العدل و المخابرات المركزية و القوات الجوية الأمريكيين إلى الاقتحام و الاختراق كما تعرض له أيضا موقع حزب العمل الإنجليزي .



وفي عام ١٩٩٧ م قدرت وكالة المباحث الفيدرالية الأمريكية و يرمز لها بـ ( F B I ) تعرض حوالي ٤٣ % من الشركات التي تستخدم خدمة الإنترنت لمحاولات اختراق تتراوح بين ( ٣ - ٥ ) مرات خلال سنة واحدة .  
• ( WILSON - 2000 )

و محاولات الاختراق و الاقتحام لا يقوم بها المحترفون فقط و إنما قد يقوم بها الهواة أيضا من باب إثبات الذات و القدرة على القيام بتلك المحاولات بنجاح مثلهم في ذلك مثل المحترفين و مثال ذلك ما حدث مع مراهقة في الخامسة عشر من عمرها عندما قامت بمحاولة اختراق إلى الصفحة العنكبوتية الخاصة بقاعدة عسكرية للغواصات الحربية بسنغافورة و كان تبريرها لما قامت به أنها قد ملت من مشاهدة التليفزيون ففكرت في شئ آخر تقوم به يبدد ما تشعر به من ملل ( KOERNER - 1999 ) •

ومرة أخرى أثناء حرب الخليج الأولى عندما اتضح لوكالة المباحث الفيدرالية الأمريكية ( F B I ) عندما اجروا تحقيقا حول تسلل أشخاص إلى الصفحة العنكبوتية الخاصة بإحدى القواعد العسكرية الأمريكية و كانت الشكوك في البداية تسجه إلى أن التسلل قد حدث من إرهابيين دوليين محترفين ألا انه قد اتضح في النهاية أن المتسلل ما هو إلا مراهقان تسللا عن طريق جهاز الكمبيوتر من منزلهما ( WILSON - 2000 ) •

و في عام ١٩٩٧ م قام مراهق بالتسلل إلى نظام مراقبة حركة الملاحة الجوية في مطار ( MASSACHUSETTS ) مما أدى إلى تعطيل نظام الملاحة الجوية لمدة ستة ساعات و بالرغم من فداحة الضرر الذي تسبب فيه هذا التسلل ألا أن عقوبة المراهق الذي قام بالتسلل اقتصررت على وضعه نحن المراقبة لمدة سنتين فقط ( WILSON - 2000 ) •



و هنا نجد أمرا هاما يعمل على كثرة عدد من يحاولون اختراق أجهزة الحاسبات الآلية الخاصة بالمطارات و القواعد العسكرية و البنوك و ما إلى ذلك من عمليات الاختراق التي تتم لعدد كبير من أجهزة الحاسبات الآلية الخاصة بمناطق و أماكن حساسة لا تتحمل ذلك العبث بأجهزتها .

أن عدم وجود العقوبة القانونية الشديدة التي تجعل من يريد القيام بعملية اختراق يفكر ألف مرة و مرة قبل القيام بتلك المحاولة هو العامل الأهم في زيادة تلك العمليات و عدم قدرة الأجهزة الأمنية على محاولة الحد منها لان القانون لا يساعدها على القيام بالواجبات المنوط بها القيام بها و يبقى أمامها شئ واحد فقط يعد هو سبيلها الوحيد لمحاولة وقف هذا السيل من محاولات الاختراق ألا وهو محاولة الوقوف أمام هؤلاء المتسللين بمحاولة القيام بإجراءات إلكترونية متقدمة و شديدة التعقيد في محاولة منهم لجعل القيام بمحاولة تسلل هي من الأمور الصعبة جدا و التي لا يستطيع حتى المحترفين القيام بها .

و قد أوضحت دراسة أجريت عام ١٩٧٩ م على عدد ( ٥٨١ ) طالب جامعي أمريكي أن نسبة ٥٠ % منهم قد اشترك في أعمال غير نظامية أثناء استخدام الإنترنت خلال ذلك العام و أن ( ٤٧ ) طالب أو ما نسبته ٧,٣ % سبق وان قبض عليه في جرائم تتعلق بالحاسب الآلي وان ٧٥ طالبا منهم أو ما نسبته ١٣,٣ % منهم قبض على أصدقائهم في جرائم تتعلق أيضا بالحاسب الآلي ( SKINNER & FREEMAN . 1997 )

ومن المعروف أن عدد جرائم من تلك النوعية قد تضاعفت في الولايات المتحدة الأمريكية ففي عام ١٩٩٩ م تحرت وكالة المباحث الفيدرالية ( F B I ) عن ( ٨٠٠ ) حالة تتعلق بالتسلل ( HACKING ) وهو ضعف عدد الحوادث التي

قامت بالتحري عنها في العام السابق أي عام ١٩٩٨ م أما الهجوم على شبكات الحاسب الآلي على الإنترنت فقد تضاعف هو الآخر ألا أن نسبة الزيادة قد بلغت ( ٣٠٠ % ) في ذلك العام أيضا وهي زيادة رهيبية .

و في محاولة من قيام الجهات الأمنية المسؤولين عن أمن الحاسبات الآلية ببناء هذا الجدار الأمني الإلكتروني و بمساعدة تقنية و فنية من المتسللين أنفسهم بل و المحترفين منهم على وجه الخصوص .

فعلى سبيل المثال يرسل مسؤولي أمن الحاسبات الكثير من الأسئلة التي نطق بأحدث سبل الحماية لغرف الدردشة الخاصة بمواقع المتسللين أو ما تعرف باسم ( HACKER INTERNET CHAT ROOM ) و لطلب نصائح تقنية حول أحدث سبل الحماية .

بل أن الأكثر من ذلك أن وكالة المباحث الأمريكية ( F.B.I ) استعانت أيضا بخبراء في التسلل ( HACKERS ) لتدريب منسوبي الوكالة على طرق التسلل ( HACKING ) لتنمية خبراتهم و قدراتهم في هذا المجال و ليستطيعوا مواكبة خبرات و قدرات المتخصصين و المحترفين من المتسللين ( HACKERS ) ومنهم أحد أشهر المتسللين في العالم و يدعى ( BRIAN MARTIN ) و هو مشهور باسم ( JERICHO ) وهم متهم حاليا بتهمة التسلل و العبث بمحتويات الصفحة الرئيسية لصحيفة ( NEW YORK TIMES ) على شبكة الإنترنت ( STAFF . 2000 . APRIL 2 ) . وقد أكدت وحدة الخدمات السرية الأمريكية ( THE U S SECRET SERVICE ) أن الجرائم المنظمة قد بدأت في الاتجاه نحو استغلال التسلل ( HACKING ) للحصول على المعلومات اللازمة لتنفيذ مخططاتها الإجرامية ( THOMMAS . 2000 ) .

وفى خبر نشرته صحيفة ( لوس أنجلوس تايمز ) أوضح أن متسللين قاموا باقتحام نظام الحاسب الآلي الذي يتحكم في تدفق أغلب الكهرباء في ولاية كاليفورنيا الأمريكية .

حذرت مصادر أمنية من ظهور تقنية جديدة تتيح للمخربين اختراق أكثر الأجهزة الحاسوبية حصانة عن طريق تطوير جيل جديد من الملفات التجسسية التي بإمكانها التحايل على أنظمة الحماية المثبتة في نسبة كبيرة من الأجهزة الشخصية المرتبطة بالإنترنت.

وصدر التحذير من جماعة أمنية ونشر موقع [WWW.PCWORLD.COM](http://WWW.PCWORLD.COM) أجزاء منه وتضمن معلومات غاية في الخطورة تشير إلى قيام ألها كرز بتطوير تقنية جديدة تمكن أحصنة طروادة أو الملفات التجسسية TROJAN من اقتحام الأجهزة الشخصية حتى في ظل برامج وجود حماية كبرامج الجدران النارية FIER WALL عن طريق الاستفادة من ثغرات أمنية معروفة في متصفح الإنترنت - إنترنت اكسبلورر - في إصداراته الجديدة.

وقال التقرير أن الفكرة التي تم تطويرها باستخدام تقنيات تخريبية متقدمة تتمثل في قيام الملف التجسسي بفتح ثغرة في متصفح الإنترنت وتسخيرها لأي مخترق يمتلك البرامج الخاصة بذلك لتمكنه من العمل خفية في الجهاز المصاب حتى في ظل وجود برامج الجدران النارية FIER WALL التي لن تتعرف عليه مشيرا إلى أنه يمكنه استخدام ملقم خارجي لا يمكن للجدار الناري تحديده في حالة تم القيام بمسح الجهاز المصاب لأنه يعمل باستخدام ملقمات تتيح إخفاء هوية مستخدميها.

و أضاف التقرير أن التقنية الجديدة ستتيح للها كرز اختراق أي جهاز حتى ولو كان يتضمن جدارا ناريا قويا مشيرا إلى أن التقنية تمثل نجاحا لجهود ألها كرز الذين قاموا بتطوير المزيد من البرامج التي تتجاوز إمكانات جدران الحماية

السنارية والتي تقوم في الغالب بصد هجماتهم ودعا التقرير شركة مايكروسوفت إلى قيامها بسد الثغرات الأمنية في متصفحتها الحالية والسابقة مطالبا المستخدمين أنفسهم بالقيام بنفس المهمة لتحسين متصفحاتهم التي تعد بمثابة جواز السفر في العالم الافتراضي.

## ٢ - الإغراق بالرسائل

لم تتوقف محاولات المتسللين عن التوصل إلى طرق جديدة يمكنهم من خلالها العمل على الأضرار بأجهزة الحاسبات الآلية **COMPUTERS** دونما أي استفادة إلا إثبات تفوقهم في ذلك ومن تلك الطرق التي توصلوا إليها طريقة الإغراق بالبريد الإلكتروني و تلك الطريقة تعني إرسال كم هائل من الرسائل **SENDING A LOT OF MESSAGES** عبر البريد الإلكتروني **E \_ MAIL** لأجهزة الحاسبات الآلية **COMPUTERS** المراد العمل على تعطيلها و وتوقفها عن العمل و بالفعل فإن تلك الرسائل الكثيرة والتي لا تعنى شئ على الإطلاق .

فتلك الرسائل **MESSAGES** قد تكون محملة بملفات **FILES** كبيرة الحجم لمجرد التأثير على الجهاز نظرا لصغر المساحة المحددة للبريد الإلكتروني **E \_ MAIL** في معظم الأحيان - و التي تصل لجهاز الحاسب الآلي **COMPUTERS** مرة واحدة و في وقت واحد تقريبا تعمل على توقفه عن العمل على الفور نظرا لما تسببه من ملء منافذ الاتصال ( **COMMUNICATION - PORTS** ) و كذلك ملء قوائم الانتظار ( **QUEUES** ) و بمجرد توقف تلك الأجهزة **COMPUTERS** عن العمل تنقطع بالتالي الخدمة التي تؤديها تلك الأجهزة .



## VIRUSES

### ٣ - الفيروسات

الفيروس هو برنامج مثل أي برنامج آخر موجودا على جهاز الحاسب الآلي  
VIRUSES IS A PROGRAM LIKE ANY ANOTHER  
PROGRAM ON THE COMPUTER و لكنها مصممة بحيث يمكنها  
التأثير على كافة البرامج الأخرى الموجودة على جهاز الحاسب الآلي سواء بأن  
تجعل تلك البرامج الأخرى نسخة منها أو أن تعمل على مسح كافة البرامج  
الأخرى من على جهاز الحاسب الآلي و بالتالي تعطلها عن العمل .  
و أما عن بدأ عملها فبدأ عملها يتحدد طبقا لأسلوب تصميمها فقد تبدأ تلك  
الفيروسات العمل بمجرد فتح الرسالة الموجودة بها و التي وصلت عن طريق  
البريد الإلكتروني و قد تبدأ العمل بمجرد تشغيل البرنامج الموجودة عليه في  
الجهاز و هكذا .

### سبب التسمية

سمي الفيروس ( VIRUS ) بهذا الاسم لتشابه آلية عمله مع تلك  
الفيروسات التي تصيب الكائنات الحية بعدد من الخصائص كخاصية الانتقال  
بالعدى و كونه كائنا غريبا يقوم بتغيير حالة الكائن المصاب إضافة إلى الضرر  
الذي يتسبب فيه أن يتم العلاج بإزالته .

### أنواع الفيروسات

## TYPES OF VIRUS

و يمكننا تقسيم تلك الفيروسات إلى أنواع هي :



- النوع الأول

فيروسات الجزء التشغيلي للاستطاعة كفيروس ( BRAIN ) و ( NEWZELAND )

- النوع الثاني

الفيروسات المتطفلة كفيروس ( CASCADE ) و ( VIENNA )

- النوع الثالث

الفيروسات المتعددة الأنواع كفيروس ( SPANISH - TELECOM ) و ( FLIP )

- النوع الرابع

الفيروسات المصاحبة للبرامج التشغيلية ( EXE ) سواء على نظام الدوس أو نظام الويندوز

و يمكن تقسيم الفيروسات على أساس آخر وهو المكان المستهدف بالإصابة داخل جهاز الكمبيوتر و على هذا الأساس يتم تقسيم الفيروسات إلى ثلاثة أنواع هي :

النوع الأول :	فيروسات قطاع الإقلاع ( BOOT SECTOR )
النوع الثاني :	فيروسات الملفات ( FILE INJECTORS )
النوع الثالث :	فيروسات الماكرو ( MACRO VIRUS )

و هناك تقسيم ثالث يمكن تقسيم الفيروسات إليه ولكن في هذا التقسيم يتم تقسيم الفيروسات إلى

١ - فيروسات الإصابة المباشرة

٢ - الفيروسات المقيمة

### ٣ - الفيروسات المتغيرة

#### ١ - فيروسات الإصابة المباشرة DIRECT ACTION

و هي التي تقوم بتنفيذ مهمتها التخريبية فور تنشيطها

#### ٢ - الفيروسات المقيمة STAYING

و هي التي تظل كامنة في ذاكرة الجهاز و تنشط بمجرد أن يقوم المستخدم بتنفيذ أمر ما و معظم الفيروسات تندرج تحت هذا النوع

#### ٣ - الفيروسات المتغيرة POLYMORPHS

و هي الفيروسات التي تقوم بتغيير شكلها باستمرار أثناء عملية التكاثر حتى تضلل برامج مكافحة الفيروسات التي قد تستخدم للقضاء عليها

و من جرائم إرسال فيروسات قيام شخص أمريكي يدعى ( ROBERT MORRIS ) بإرسال دودة حاسوبية بتاريخ ٢ / ٨ / ١٩٨٨ م عبر الإنترنت و قد كرر الفيروس ( VIRUS ) نفسه عبر الشبكة بسرعة فائقة فاقت حتى تصور مصممها نفسه و قد أدى ذلك إلى تعطيل ما يقارب من ( ٦٢٠٠ ) حاسب إلى مرتبط بالإنترنت و قد قدرت الأضرار التي لحقت بتلك الأجهزة بمئات الملايين من الدولارات و لو قدر لمصمم الفيروس أن يصممه ليكون اشد ضررا لكان قد لحقت أضرارا أخرى لا يمكن حصرها بتلك الأجهزة و قد حكم عليه بالسجن ثلاث سنوات بالرغم من انه دافع عن نفسه بأنه لم يكن يقصد إحداث كل هذا الضرر .

المصدر : موقع

[HTTP://WWW.MINSHAWI.COM/INTERNETCRIM](http://WWW.MINSHAWI.COM/INTERNETCRIM)

## كيفية اقتحام الجهاز

- لتنم عملية التسلل لابد من زرع حصان طروادة و يتم زرعها بعدة طرق :
- ١ - يرسل عن طريق البريد الإلكتروني كملف ملحق حيث يقوم الشخص باستقباله و تشغيله و قد لا يرسل لوحده حيث من الممكن أن يكون ضمن برامج أو ملفات أخرى .
  - ٢ - عند استخدام برنامج المحادثة الشهير ( I C Q ) و هو برنامج محادثة أنتجته إسرائيل
  - ٣ - عند تحميل برنامج من أحد المواقع غير الموثوق بها
  - ٤ - مجرد كتابة كوده على الجهاز نفسه
  - ٥ - في حالة اتصال الجهاز بشبكة داخلية أو شبكة إنترنت
  - ٦ - يمكن نقل البرنامج أيضا بواسطة برنامج ( F T P ) أو ( TELNET )
  - ٧ - كما يمكن الإصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكرو الموجود في برامج معالجة النصوص

## WORMS

## الديدان

### DEFINITION

### تعريفها

هي برامج صغيرة قائمة بذاتها و غير معتمد على غيرها و صنعت للقيام بأعمال تدميرية أو بغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم على شبكة الإنترنت أو لإلحاق الضرر بهم أو بالمتصلين بهم و تلك الديدان تتميز بسرعة الانتشار و في نفس الوقت يصعب التخلص منها نظرا لقدرتها الفائقة على التلون و التناسخ و المراوغة .

## آلية عمل الديدان

تختلف الديدان في طريقة عملها من نوع إلى آخر فبعضها يقوم بالتناسخ داخل الجهاز إلى أعداد هائلة بينما بعضها يتخصص في البريد الإلكتروني بحيث تقوم بإرسال نفسها في رسائل إلى جميع من توجد عناوينهم في دفتر العناوين الموجود بالجهاز و أنواع أخرى من الديدان تقوم بإرسال رسائل قذرة إلى بعض الموجودة عناوينهم في دفتر العناوين الموجود بالجهاز بأسم مالك البريد مما يوقعه في حرج بالغ مع من تم إرسال تلك الرسائل إليهم

و تكمن خطورة الديدان في استقلاليتها و عدم اعتمادها على أي برامج أخرى تتحقق بها مما يعطيها حرية كاملة في الانتشار السريع و مما لا شك فيه أنه توجد أنواع منها في غاية الخطورة حتى أن بعضها أصبح كابوسا مرعبا كل ملارم للشبكة و مثال ذلك تلك الدودة التي ظهرت في أكتوبر عام ٢٠٠٢ م و اشتهرت بأسم ( TANATOS ) و انتشرت انتشار النار بالهشيم و خلفت ورائها أثارا تدميرية هائلة .

من المعلوم أن أشهر وسائل انتشار الديدان هو عن طريق الرسائل الإلكترونية المفخخة و التي عادة ما تكون عناوين تلك الرسائل جذابة كدعوة لمشاهدة صور أحد النجوم أو المشاهير لذلك لابد من توخي الحذر حتى وإن كانت تلك الرسائل من مصدر معروف و موثوق به لان تلك الديدان تقوم بإرسال نفسها في شكل رسائل إلى كافة الموجودة عناوينهم على الجهاز

## كيفية الحماية من الديدان

تتم الحماية من الديدان بتركيب أحد البرامج المضادة للديدان و المتخصصة في ذلك ( WORM GUARD ) أو بتركيب أحد البرامج المضادة للفيروسات بصفة عامة .

## التكليف القانوني للجريمة

تعد جريمة التسلل أو الاختراق لأجهزة الحاسبات الآلية الخاصة بالغير هي جريمة تنطبق عليها النصوص القانونية المتعلقة بالدخول إلى ملك الغير و العبث بما به من محتويات أو تخريبها أما إذا زاد على ذلك سرقة بعض تلك المحتويات فتزداد هنا جريمة السرقة .

فتنص المادة ٣٦٩ من قانون العقوبات المصري على أن (( كل من دخل عقارا في حيازة آخر بقصد منع حيازته بالقوة أو بقصد ارتكاب جريمة فيه . . . . يعاقب بالحبس مدة لا تجاوز سنة أو بغرامة لا تجاوز ثلاثمائة جنيه مصري )) كما تنص المادة ٣٦١ من قانون العقوبات المصري على انه (( كل من اتلف عمدا أموالا ثابتة أو منقولا لا يمتلكها أو جطها غير صالحة للاستعمال أو عطلها بأي طريقة يعاقب بالحبس مدة لا تزيد على ستة اشهر أو بغرامة لا تجاوز ثلاثمائة جنيه مصري لا غير .

فإذا ترتب على الفعل ضرر مالي قيمته خمسون جنيها فأكثر كانت العقوبة الحبس لمدة لا تجاوز سنتين و غرامة لا تجاوز خمسمائة جنيه أو بإحدى هاتين العقوبتين .

و تكون العقوبة مدة لا تزيد عن خمس سنوات و لا تجاوز ألف جنيه إذا نشأ عن الفعل تعطيل أو توقيف أعمال مصلحة ذات منفعة عامة أو إذا ترتب عليه جعل حياة الناس أو أمنهم في خطر .

و يضاعف الحد الأقصى للعقوبة إذا ارتكبت الجريمة تنفيذا لغرض إرهابي )) و عليه و على اعتبار أن جهاز الحاسب الآلي هو عقار يحتفظ فيه الناس بكافة أو على الأقل بمعظم متعلقاتهم المعلوماتية الهامة بل و الكثير من أسرارهم المعلوماتية الخاصة بما يملكونه من أموال أو معلومات فهو يسرى عليه ما تم



النص عليه في المادة ٣٦٩ من قانون العقوبات المصري .  
و أيضا يعد جهاز الكمبيوتر هو أموال منقولة فالتسلل إليها و تخريبها أو  
تعطيلها عن العمل يسرى عليها المادة ٣٦١ من قانون العقوبات المصري .

### ثالثا : الجرائم المالية

تنقسم الجرائم المالية التي تتم عبر الإنترنت إلى ستة أنواع من الجرائم هي :

- ١ - جرائم السطو على أرقام البطاقات الائتمانية

- ٢ - لعب القمار

- ٣ - تزوير البيانات

- ٤ - الجرائم المنظمة

- ٥ - تجارة المخدرات

- ٦ - غسيل الأموال

### ١ - جرائم السطو على أرقام البطاقات الائتمانية

منذ أن بدأ استخدام البطاقات الائتمانية عبر شبكة الإنترنت حتى كان اللصوص  
المتسللين في أعقابها بلا هوادة فالبطاقات الائتمانية تعد نقودا إلكترونية و  
الاستيلاء عليها يعد استيلاء على مال الغير .

و نظرا لسهولة الاستيلاء على تلك الأرقام فقد تزايدت حوادث الاستيلاء عليها  
و أيضا تزايدت عمليات الابتزاز المصاحبة لارتكاب مثل تلك الجرائم و عمليات  
الابتزاز تلك تكون أما لإعادة تلك الأرقام أو لعدم نشرها أو لعدم استخدامها من  
قبل من استولى عليها .

و قد وقعت بالفعل عدة حوادث من ذلك النوع و منها قيام شخص ألماني بالدخول غير المشروع إلى أحد مزودي الخدمة و استيلاءه على أرقام البطاقات الائتمانية الخاصة بالمشاركين و من ثم بدأ في ابتزاز صاحب الخدمة بنشر تلك الأرقام أو سداد فدية مالية ألا أن الشرطة الألمانية قد نجحت في القبض على ذلك اللص المتسلل عند استلامه الفدية .

كما قام شخصان في عام ١٩٩٤ م بإنشاء موقع على شبكة الإنترنت مخصص لشراء طلبات يتم إرسالها بمجرد سداد قيمتها إلكترونياً إلا أنه كان الغرض الأساسي من إنشاء هذا الموقع هو الاستيلاء على أرقام البطاقات الائتمانية الخاصة بالمشاركين من هذا الموقع أي أن الغرض الأساسي من هذا الموقع كان النصب و الاحتيال على مرتاديه للحصول منهم طواعية على أرقام بطاقتهم الائتمانية

و قد اثبتت شبكة ( MSNBC ) عملياً مدى سهولة الحصول على أرقام البطاقات الائتمانية من شبكة الإنترنت حيث قامت بعرض قوائم تحتوى على أكثر من ٢٥٠٠ رقم بطاقة ائتمانية حصلت عليها من سبع مواقع للتجارة الإلكترونية و ذلك عن طريق استخدام قواعد بيانات متوافرة تجارياً و لم يكن ممن الصعب على أي متطفل أو متسلل استخدام تلك الوسيلة البدائية الوصول و الاستيلاء على تلك الأرقام و استخدامها في عمليات شراء يدفع الثمن فيها أصحاب البطاقات الحقيقيون .

و يتعدى الأمر المخاطر الأمنية التي يمكن أن تتعرض لها البطاقات الائتمانية الحالية فنحن الآن في بداية ثورة نقدية يطلق عليها أسم النقود الإلكترونية ( ELECTRONIC CASH ) أو ( CYBER CASH ) و التي يتنبأ لها بأن تكون مكملة للنقود الورقية أو البلاستيكية ( بطاقات الائتمان ) و

من المتوقع أيضا أن يزداد الاعتماد على هذا النوع الجديد و الحديث من النقود ( CACH ) و أن تحوز الثقة ( CONFIDENCE ) التي تحوزها النقود التقليدية هذا بجانب الأسهم و السندات الإلكترونية المعمول بها حاليا في دول الاتحاد الأوروبي حاليا و التي أقر الكونجرس الأمريكي العمل و التعامل بها عام ١٩٩٠ م .

فإذا كانت البطاقات الائتمانية الحالية تواجه كل تلك المخاطر فما الحال عند استخدام الأنواع الجديدة من النقود الإلكترونية ( ELECTRONIC CACH ) فنحن بحاجة إلى تدعيم الثقة في تلك الأنواع من النقود التي يتم استخدامها حاليا عبر شبكة الإنترنت حتى تجد الأنواع الجديدة من النقود الإلكترونية الثقة اللازمة ليتعامل بها الأفراد دون خوف من اعتداء اللصوص المتسللين إليها و إفشاء بياناتها و سرقتها .

### التكليف القانوني للجريمة

سرقة أرقام البطاقات الائتمانية تعد جريمة موازية تماما لجريمة سرقة النقود و هي جريمة منصوص عليها في كافة القوانين فجريمة السرقة هي جريمة تعد من أقدم الجرائم المعروفة على مستوى العالم و عليه فهي منصوص على تجريمها في كافة قوانين العالم .

وفي مصر تنص المادة ٣١١ من قانون العقوبات المصري على أن

(( كل من اختلس منقولا مملوك للغير فهو سارق ))

و تختلف العقوبة المقررة على جريمة السرقة بحسب وجود أي من العوامل المشددة للجريمة كوجود سلاح مع السارق أو أن تتم تلك السرقة في الليل و ما إلى ذلك من العوامل التي تعد عوامل مشددة للعقوبة .

و رغم أن تلك العوامل ليس لها محل في جريمة سرقة أرقام بطاقات الائتمان عن طريق الإنترنت إلا أن جريمة السرقة كجريمة معاقب عليها .

## ٢ - ممارسة القمار

في الماضي كان لعب القمار يستلزم وجود اللاعبين معا على طاولة ليتمكنوا من لعب القمار معا أما الآن و مع انتشار شبكة الإنترنت على مستوى العالم فقد أصبح لعب القمار اسهل و أصبح تجمع اللاعبين على مستوى العالم في مكان واحد اسهل من ذي قبل على الإطلاق فقد أصبح بإمكان اللاعبين التجمع معا عبر شبكة الإنترنت و لعب جميع أنواع القمار من خلال الشبكة .

كما أن انتشار المواقع على شبكة الإنترنت التي توفر لمثل هؤلاء اللاعبين ما يحتاجونه من برامج ليتمكنوا من لعب القمار قد زادت و انتشرت على الشبكة نظرا لان اللاعبين بات بإمكانهم اللعب و كل منهم في منزله دون أن يضطر إلى مجرد الخروج من منزله و الذهاب إلى الأماكن التي يمكنه اللعب فيها . و عليه فإن انتشار شبكة الإنترنت قد اسهم من ضمن ما اسهم فيه من السلبيات انتشار لعب القمار .

و نظرا لان القمار قد يكون مصرحا به في بعض البلاد إلا انه الأغلب الأعم من البلاد مصرح به و لكن بشكل محدود جدا و في بعض الأماكن السياحية فقط دون أن يكون مصرحا به في الأماكن العادية التي يرتادها الأغلب الأعم من أفراد الشعب نظرا لأنه يخالف تعاليم الدين في كافة البلاد العربية التي يرفض الدين الإسلامية لعب القمار و يحرمه .

و بالتالي فلعب القمار غير مصرح به حتى ولو كان عن طريق الإنترنت . و حتى في أمريكا فان لعب القمار عبر شبكة الإنترنت غير مصرح به قانونا

على الإطلاق و ليستفادى أصحاب المواقع تلك المشكلة القانونية يلجأون إلى إدارة تلك المواقع المشبوهة من خارج حدود الولايات المتحدة الأمريكية .  
ولذلك فقد بدأت الأصوات تعلوا هناك من أجل البدء في ملاحقة القائمين على تلك المواقع لمخالفتهم القانون الذي يجرم لعب القمار عبر الشبكة إلا أن الأرباح الخيالية التي يجنيها أصحاب تلك المواقع تدفعهم إلى المراوغة و الهرب من تلك الملاحقة حتى لا يغلقوا تلك المواقع التي يربحون من ورائها مليارات الدولارات من اللاعبين الذين يدخلون على مواقعهم من كافة دول العالم دونما خوف من مخالفة القانون في بلادهم .

### التكليف القانوني للجريمة

لعب القمار - بكافة أنواعه - هو من الأمور المعاقب عليها في معظم بلاد العالم و كافة البلاد الإسلامية إلا انه قد يكون مصرحا به فقد في بعض الأماكن السياحية فقط و كعامل من العوامل التي تعمل على تنشيط السياحة ؛  
و عدم قانونية لعب القمار تسرى على كافة أنواع لعبه سواء بطريقة مباشرة كالطرق المباشرة و الطرق غير المباشرة كعبه عن طريق الإنترنت .  
و في مصر تنص المادة ٢٥٢ من قانون العقوبات على انه (( كل من اعد مكانا لألعاب القمار و هيأه لدخول الناس فيه يعاقب هو و صيارف المحل المذكور بالحبس و بغرامة لا تتجاوز ألف جنيه و تضبط جميع النقود و الأمتعة في المحلات الجارية فيها الألعاب المذكورة و يحكم بمصادرتها ))  
و يسرى هذا النص على كل من انشأ موقعا على الإنترنت للعب القمار طالما كان منشأ هذا الموقع مصري أو غير مصري طالما أنشأه من مصر كما يسرى هذا النص أيضا على كل من دخل على هذا الموقع للعب القمار فيما لو استطاعت السلطات التوصل إليه .



## FORGERY OF DATA

## ٣ - تزوير البيانات

تعتبر جرائم تزوير البيانات من أكثر الجرائم شيوعاً من بين كافة أنواع الجرائم التي ترتكب سواء على شبكة الإنترنت أو ضمن جرائم الحاسب الآلي نظراً لأنه لا تخلو جريمة من الجرائم إلا و يكون من بين تفاصيلها جريمة تزوير البيانات بشكل أو بآخر .

و تزوير البيانات **FORGERY OF DATA** يكون بالدخول - سواء بطريقة شرعية أو غير شرعية - على قاعدة البيانات **DATABASE** الموجودة و تعديل تلك البيانات سواء بإلغاء بيانات موجودة بالفعل أو بإضافة بيانات لم تكن موجودة من قبل .

و من تلك الحوادث التي تم فيها الدخول على قاعدة البيانات **DATABASE** بطريقة شرعية تلك الحادثة التي وقعت في ولاية كاليفورنيا الأمريكية حيث عمدت مدخلة البيانات بنادي السيارات و بناء على اتفاق مسبق بينها و بين صديقها - لص سيارات - بتزوير البيانات **FORGERY OF DATA** الخاصة بملكية السيارات و المسجلة في الحاسب الإلكتروني بحيث تصبح باسم صديق الفتاة و هو أحد لصوص السيارات و الذي يعمد إلى سرقة السيارة و بيعها و بالتالي عندما يتقدم مالك السيارة الحقيقي للإبلاغ عن سرقة سيارته و بالبحث في قاعدة البيانات **DATABASE** بالحاسب الإلكتروني يتضح عدم وجود سجلات للسيارة باسمه و بعد أن يقوم صديق الفتاة ببيع السيارة تقوم ذات الفتاة بإعادة تسجيل السيارة باسم صاحبها الأصلي أي إعادة البيانات كما كانت عليه دون أي تعديل و قد كانت تلك الفتاة تتقاضى عن كل عملية من تلك العمليات مبلغ مائة دولار لا غير و قد استمرت في عملها هذا إلى أن تم اكتشافها و القبض عليها .

تلك الجريمة هي مثال واضح و صريح على جرائم تزوير البيانات **FORGERY OF DATA** و ما تسببه من ضياع الحقوق و زيادة جرائم السرقة التي تتزايد بنسب كبيرة بعد استخدام عمليات تزوير البيانات في تسهيلها فعمليات تزوير البيانات يكون الغرض الأساسي منها في معظم الأحيان هو تسهيل عمليات السرقة التي لا يمكن إتمامها إلا بتزوير البيانات .

وفى حادثة أخرى قام مرتكبها بالدخول على قاعدة البيانات **DATABASE** بطريقة شرعية أيضا حيث قام مشرف تشغيل الحاسب بأحد البنوك الأمريكية أيضا بعملية قام من خلالها بتزوير بيانات **FORGERY OF DATA** حسابات أصدقائه في البنك بحيث تزيد أرصدتهم عما هي عليه و من ثم يتم سحب تلك الأرصدة من قبل أصدقائه بعد زيادتها و قد نجح في ذلك عدة مرات و قام أصدقائه بسحب الكثير من الأموال و كان هذا الشخص ينوى التوقف قبل موعد المراجعة الدورية لحسابات البنك إلا أن طمع أصدقائه أجبره على الاستمرار في ارتكاب تلك العمليات الإجرامية إلى أن تم القبض عليه .

هذا من جهة و من جهة أخرى فإن اتجاه الحكومات على مستوى العالم إلى الاتجاه إلى الحكومات الإلكترونية **ELECTRONIC GOVERNMENT** و كذلك انتشار التجارة الإلكترونية **ELECTRONIC COMMERCE** عبر دول العالم و صدور القوانين المنظمة له سيزيد من فرص ارتكاب تلك الجرائم **CRIMES** و في نفس الوقت سيعمل على إضعاف فرصة القبض على مرتكبي تلك الجرائم فالحكومات الإلكترونية هي المناخ الأنسب لارتكاب مثل تلك الجرائم .

فالارتباط الذي سيتم فيما بين البنوك و الشركات و الحكومات بشبكة الإنترنت ستعمل على تهيئة المناخ أكثر و أكثر لتنفيذ مثل تلك الجرائم .

## التكييف القانوني للجريمة

جريمة التزوير هي الأخرى من الجرائم المنصوص على تجريمها في كافة القوانين ولا توجد أي دولة لا تجرم قوانينها عمليات التزوير .  
فجريمة التزوير لا توجد دولة لا تجرمها بل ولا تشدد في العقوبات المقررة على ارتكابها .

وفي مصر فقد أقر المشرع المصري الباب السادس عشر كاملا في قانون العقوبات للنص على تجريم عمليات التزوير أيا كان مرتكبها و سواء ارتكبت على توقيع أو بيان أو خلافه و قد نص المشرع المصري على تجريمها بداية من المادة ٢٠٦ و حتى المادة ٢٢٧ .

## رابعاً : الجرائم المنظمة

عصابات المافيا هم أشهر من قام بالجرائم المنظمة فعلى الرغم من أن هناك الكثير من العصابات على مستوى العالم تقوم بالجرائم المنظمة ذات الخبرة في التنفيذ و الخطيرة التأثير إلا أن عصابات المافيا هي الأشهر من بين تلك العصابات .

و شبكة الإنترنت كانت من أهم الوسائل التي ساعدت كثيرا أعضاء عصابات المافيا على تطوير و تحسين عملياتهم على مستوى العالم إذ أنها عملت على إلغاء حاجز الزمان و المكان من أمامهم فأصبحت عملياتهم أكثر تطورا و اعظم تأثيرا على مستوى العالم حتى أن تلك العصابات قد أقامت لها مواقع على شبكة الإنترنت لتتفادى القوانين ففي بلد ما قد يمنع القانون فعل ما بينما في بلد آخر قد لا يمنع القانون بها نفس الفعل .

ان القدرات والفرص التي تؤمنها شبكة الإنترنت طورت العديد من النشاطات التجارية المشروعة من خلال زيادة سرعة وسهولة ومجالات إجراء المعاملات إضافة الى تخفيض الكثير من النفقات واكتشف المجرمون أيضاً أن شبكة الإنترنت تستطيع أن تؤمن فرصاً جديدة وفوائد متضاعفة للأعمال غير المشروعة فالجانب المظلم من الإنترنت لا يشمل فقط الاحتيال والسرقة ونشر المواد الإباحية وشبكات المنحرفين جنسياً ممن يستهدفون الأحداث بل أيضاً منظمات الاتجار بالمخدرات والمنظمات الإجرامية التي تركز على استغلال ما توفره الشبكات الإلكترونية من تسهيلات وفرص أكثر مما تركز على تعطيل عمل الشبكات كما يفعل الآخرون المهتمون بهذا الأمر.

و من جهة أخرى فكون شبكة الإنترنت يمكن استخدامها من دون معرفة المستخدم فهذا يجعل منها قناة مثالية وجهازاً مثالياً لتنفيذ العديد من نشاطات الجريمة المنظمة ومفهوم عالم الجريمة السري يعني أنه تسود هذا العالم الضبابية او نقص الشفافية فالسرية تشكل عادة جزءاً رئيسياً من استراتيجية الجريمة المنظمة وشبكة الإنترنت توفر فرصاً ممتازة للمحافظة على هذه السرية إذ يمكن إخفاء الأعمال وراء حجاب من الإغفال قد يتراوح مداه من استعمال معايير علم التحكم الإلكتروني إلى جهود متطورة لإخفاء المسار التي تتبعه المعاملات عبر الإنترنت لتصل إلى مقصدها .

تتناول الجريمة المنظمة في الأساس السعي للإفادة المادية أو تحقيق الأرباح من خلال مواصلة العمل بوسائل جرمية ولذا كما تستعين الشركات العادية بشبكة الإنترنت بحثاً عن فرص جديدة لتحقيق الأرباح كذلك تفعل المنظمات الإجرامية والمنظمات الإجرامية ليست اللاعبات الوحيدات في أسواق الأعمال غير المشروعة ولكنها تكون في أحيان كثيرة أهم اللاعبين، على الأقل بسبب تمتعها



بقُدرة أكبر على المنافسة التي يوفرها لها تمكّنها من التهديد بأعمال العنف بالإضافة إلى ذلك تميل المنظمات الإجرامية إلى مهارة كبيرة في اكتشاف واستغلال فرص القيام بأعمال ومشاريع جديدة غير مشروعة في هذا السياق توفر الإنترنت والنمو المتواصل للتجارة الإلكترونية مجالات هائلة جديدة لتحقيق أرباح غير مشروعة .

خلال السنوات القليلة الماضية ازدادت حنكة ومهارة مجموعات الجريمة المنظمة وتجارة المخدرات فمثلاً اتبعت المنظمات الكولومبية لتجارة المخدرات الممارسات التي تقوم بها الشركات العادية لتنويع الأسواق والمنتجات واستغلت أسواقاً جديدة في أوروبا الغربية ودول الاتحاد السوفيتي السابق وأخذت المنظمات الإجرامية وتجار المخدرات تزيد من توظيف اختصاصيين ماليين لإدارة شؤون غسل الأموال أضاف هذا العمل طبقة إضافية عازلة حول عملية غسل الأموال بينما يتم استخدام خبراء قانونيين وماليين عارفين بخفايا المعاملات المالية لتوفير ملاذات آمنة في أماكن ومؤسسات تعمل بطريقة الأوف شور وبالمثل لا تحتاج الجريمة المنظمة إلى تطوير خبرة فنية في مجال الإنترنت فبإمكانها أن تستخدم أشخاصاً من الخبراء في عمل الشبكة واستغلال مكامن الضعف فيها لتنفيذ المهمات الموكلة إليهم بفعالية وكفاءة إما من خلال منحهم مكافآت سخية أو من خلال تهديدهم بما لا تحمد عقباه إذا لم يفعلوا أو من خلال مزيج من الأمرين معاً .

تكون عادة لمجموعات الجريمة المنظمة قاعدة عمل في الدول الضعيفة التي تؤمن ملاذاً آمناً تستطيع من خلاله ممارسة عملياتها العابرة للحدود الجغرافية وفي الواقع يوفر هذا الأمر قدراً إضافياً من الحماية من تطبيق القانون ويمكن تلك المجموعات من ممارسة نشاطاتها بأقل قدر من المخاطر وتتلاءم الصفات



المتأصلة للإنترنت كشبكة تتخطى حدود البلدان مع هذا النمط من النشاط الإجرامي ومع الجهد الساعي إلى تحقيق أقصى الأرباح ضمن درجة مقبولة من المخاطر ففي العالم الافتراضي أي في عالم الشبكات الإلكترونية لا توجد أي حدود وبشكل ذلك مزية تجعل النشاط الإجرامي عملاً جذاباً للغاية عندما تحاول السلطات المختصة مراقبة هذا العالم الافتراضي تبدو أمامها حدود البلدان ومناطق الصلاحيات واسعة جداً ما يجعل التحقيق في الجرم بطيئاً جداً في أحسن الأحوال أو مستحيلًا في أسوأ الأحوال .

و يوجد على شبكة الإنترنت INTERNET حوالي ٢٥٠ مائتين و خمسون موقعا LOCATIONS خاصا بأعضاء عصابات المافيا و بعصابات المافيا نفسها و تلك العصابات تستغل تلك المواقع في إرسال خططها و تعليماتها إلى أعضائها في كافة بلاد العالم بل أن بعض تلك المواقع يستغل في استقبال أعضاء جدد يريدون الانضمام إلى عالم عصابات المافيا كما أن هناك مواقع أخرى ANOTHER LOCATIONS سمح للزوار بتصفحه لمعرفة عالم عصابات المافيا عن قرب إلا أن معظم تلك المواقع غير مسموح بالدخول عليه إلا للأعضاء فقط .

و الجريمة المنظمة موجودة من فترة زمنية طويلة أي أنها لم تعتمد على التقدم التقني MODERN TECHNIQUES الحالي في تكوينها أو إنشائها إنما هي قد استغلت هذا التقدم التقني في تقوية الروابط فيما بين أعضائها و كذلك في تسهيل عملية توصيل الأوامر و التعليمات إلى أعضائها بصورة مشفرة و بالتالي دون قلق من أي عملية تعقب قد يقوم بها أي جهاز قانوني محلي أو دولي لأعضائها أو لقياداتها .

و بعض المتخصصين في مجال الجريمة المنظمة يربط بينها و بين الإرهاب

على أساس أن أساس عمل كلاهما هو إفشاء الخوف و الترويع فيما بين الناس كما أن هناك توافق كبير جدا في طريقة العمل و أساليب التنفيذ مما أدى بهؤلاء الخبراء إلى الاعتقاد إلى وجود تناسق كبير و تخطيط مشترك فيما بين كل من أعضاء منظمات الجرائم المنظمة و الإرهابيين فالإرهابيين يستفيدون من خبرة هؤلاء الأشخاص في تنفيذ مخططاتهم و العكس صحيح فأعضاء منظمات الجرائم المنظمة يستفيدون من الإرهابيين الأموال الطائلة منهم مقابل تنفيذ مخططاتهم .

### التكييف القانوني للجريمة

في الكثير من الدول تم مواجهة تلك العصابات المنظمة و الذين يقومون بارتكاب الجرائم الكبرى من خلال تشريعات خاصة تم وضعها لمواجهة تلك العصابات . الجريمة المنظمة لم تكن ضمن الجرائم المعروفة في الماضي و عليه فلا توجد أي من القواعد القانونية في مصر و التي يمكن أن تجرمها على أساس أن مرتكب تلك الجريمة هي عصابة منظمة إلا انه يمكن تجريم أي جريمة ترتكب على أساس انها جريمة قد ارتكبت من قبل عدد من الأشخاص و يتم العقاب فيها على أساس أنها ارتكبت من عدد من الأشخاص دون أن يكون لكون مرتكبها إحدى العصابات المنظمة عاملا مشددا في العقاب .

### خامسا - تجارة المخدرات

## TRAFFICKING OF DRUGS

تعد تجارة المخدرات هي أحد أهم و اخطر أنفسهم التجارة المحرمة على مستوى العالم و يأتي بعدها تجارة الرقيق الأبيض ثم تجارة السلاح .

فتجارة المخدرات هي أكثر أنفسهم التجارة المحرمة انتشارا على مستوى العالم و لم تفلح كافة الجهود المبذولة على مستوى العالم إلا في تقليلها دون القدرة على منعها نهائيا نظرا لوجود بعض دول العالم التي تتركز فيها تصنيع و تهريب تلك المخدرات إلى باقي دول العالم و لما تدره تلك التجارة على العاملين فيها من ربح وفير .

وقد كان تجار المخدرات يلاقون صعوبات كثيرة في الاتفاق على عمليات التهريب على مستوى العالم إلا أنه و بعد التطور التكنولوجي الكبير على مستوى العالم و المتمثل في انتشار شبكة الإنترنت فقد استغل مصنعي و مهربي المخدرات شبكة الإنترنت و استخدموها في الاتفاق على عمليات تهريب المخدرات من بلد إلى آخر .

إلا أن الإنترنت قد ساهمت أيضا في الترويج لتناول المخدرات و هو نشاط آخر قام به تجار المخدرات على مستوى العالم ليزيدوا من السوق الاستهلاكية و الطلب على منتجاتهم .

و في تقرير نشرته شبكة CNN الإخبارية ( WWW.CNN.COM ) ذكرت فيه قيام السلطات الاتحادية و المحلية في عدد من الولايات الأميركية بحملة واسعة بهدف تعقب مروجي المخدرات الذين يوزعون العقار المخدر المسمي GHB عبر الشبكة الإلكترونية ( الإنترنت - INTERNET ) وألقت القبض على العشرات منهم في مختلف المدن الأميركية وذلك في محاولة من السلطات في الحد من انتشار هذا العقار المخدر لما له من آثار مدمرة على الجهاز العصبي لمن يتعاطاه .

وفي أول حملة من نوعها قام المحققون بما يزيد عن ١٥٠ حملة تفتيش في أكثر من ٧٠ مدينة أميركية اعتقل فيها العديد من موزعي المخدرات الذين طوروا في أساليب نشاطهم الممنوع قانونا و أصبحوا يستخدمون تكنولوجيا

العصر الإنترنت لتوزيع بضائعهم المخدرة .

وقال مصدر في السلطات الاتحادية في الولايات المتحدة الأمريكية أن الحملة التي استغرقت عامان تقريباً تستهدف مبدئياً خمسة و عشرون من تجار المخدرات الذين يديرون تجارتهم عبر شبكة الإنترنت INTERNET الخاصة بهم والتي تمكن الزبائن من الدخول إلى الموقع وتحديد طلباتهم من مخدر ( GHB ) والأنواع المخدرة الأخرى التي يتاجرون فيها و التي ترسل إليهم عبر البريد .

وشارك قسم مراقبة البريد الأميركي ودائرة الجمارك ومكتب التحقيقات الفيدرالية الأمريكي ( F P I ) في تلك الحملة التي قادت إلى الكشف عن هؤلاء الأشخاص الذين يتاجرون في المخدرات عبر شبكة الإنترنت INTERNET و كذلك عن المواقع SITES التي يستخدمونها في نشاطهم المشبوه .

و ( GHB ) هو عقار مخدر عبارة عن خليط يتكون من مواد كيميائية صناعية وكان الكونغرس الأميركي قد اصدر قانوناً بتحريمها قبل عدة سنوات ويعمل هذا العقار المسمى ( GHB ) و كذلك مشتقاته 1K4 BD , GBL كعامل مؤثر على النظام المركزي للأعصاب مما يتسبب في الشعور بالدوار والغثيان و الدوخة وعدم القدرة على التركيز و قد قدرت الأجهزة الأمنية الأمريكية أن هذا العقار المخدر و المسمى عقار ( GHB ) و كذلك مشتقاته قد تسببت في وفاة أكثر من اثنان و سبعون شخصاً وفقاً للأوراق الرسمية .

وتحاول الأجهزة الأمنية والحكومية الأمريكية عقد دورات تثقيفية تهدف لتحذير الجميع بصفة عامة و النساء بصفة خاصة من الوقوع في فخ المروجين الذين يخلطون المواد المخدرة بالمشروبات .

## التكليف القانوني للجريمة

تعد جريمة الاتجار في المخدرات إحدى أقدم الجرائم المنصوص على تجريمها في كافة قوانين دول العالم بل والأكثر من ذلك أن تصنيعها أو زراعة أحد النباتات التي تستخرج منها أو توزيعا أو إخفائها أو أي أعمال من الأعمال المتصلة بما تم ذكره هو عمل مجرم و مشددة عقوبة القيام به .

و في مصر أيضا تعد جريمة الاتجار في المخدرات من الجرائم المنصوص على تجريمها بل أن جمهورية مصر العربية قد شددت في عقاب من يجلب المخدرات من الخارج محاولا إدخالها مصر بالإعدام شنقا متى ثبتت التهمة في حقه .

## سادسا - غسل الأموال

غسل الأموال يعني في أبسط صوره هو تحويل المصدر غير المشروع للأموال إلى مصدر مشروع فمثلا تحويل الأموال الناتجة من عمليات غير مشروعة كتجارة المخدرات إلى أموال مصدرها مشروع كتجارة السيارات مثلا .

و مصطلح غسل الأموال هو مصطلح حديث إلى حد ما و قد بدأ استخدام هذا المصطلح في الولايات المتحدة الآلي عام ١٩٣١ م حيث تمت محاكمة أحد زعماء المافيا و مصادرة أمواله على أساس أن مصدرها هو تجارة غير مشروعة ( تجارة المخدرات )

و نحن نرى انه يمكن تعريف مصطلح غسل الأموال بأنه : -

( تحويل مصدر الأموال غير المشروع إلى مصدر مشروع )

و قد أعطت شبكة الإنترنت عدة مميزات لمن يقومون بعمليات غسل الأموال منها السرعة الشديدة و تخطي الحواجز الحدودية بين الدول و تفادي القوانين



التي قد تضعها بعض الدول و تعيق نشاطهم وكذلك تشفير عملياتهم مما يعطيها قدر اكبر من السرية .

و أيضا كان انتشار التجارة الإلكترونية الإلكترونية SIGNATURE ELECTRONIC عبر شبكة الإنترنت INTERNET خير المعين لهؤلاء القائمين على عمليات غسيل الأموال فالتجارة الإلكترونية و انتشارها عبر أنحاء العالم اجمع قد ساعد كثيرا في عمليات غسيل الأموال نظرا لسرعة الاتفاق على الصفقات و إتمامها من خلاله دون أن تكون في معظم الأحيان تحت رقابة قانونية صارمة بل انه في حالة وجود رقابة قانونية يكون من الممكن تفادي تلك الرقابة و إتمام تلك الصفقات عبر الاتفاق على خطوات و ترتيبات تنفيذا عبر الإنترنت و بطريقة تشفير معقدة لا يمكن حلها و بالتالي لا يمكن من خلالها معرفة كيفية إتمام تلك الصفقات .

كذلك ساهمت بعض الجرائم التي ترتكب عبر الإنترنت INTERNET CRIMES مثل تزوير البيانات FORGERY OF DATA و المواقع الافتراضية ( الغير حقيقية ) تعد أيضا من العوامل المساعدة التي وفرتها شبكة الإنترنت للقائمين على عمليات غسيل الأموال .

### التكليف القانوني للجريمة

تعتبر جريمة غسيل الأموال هي من الجرائم الحديثة و قد قامت العديد من الدول أما بتعديل نصوصها لتستوعب تجرين تلك الجريمة الجديدة أو بتشريع نصوص جديدة تجرمها .

وفى مصر تم تشريع قانون جديد يجرم جريمة غسيل الأموال و يعاقب عليها بأشد العقوبة نظرا لما تسببه من سمعة سيئة للبلاد و تقويض الاقتصاد الوطني المصري .

## سابعاً : المواقع المعادية

مصطلح المواقع المعادية أيضاً هو مصطلح حديث بدأ استخدامه بعد هذا التطور التكنولوجي الذي نعيشه حالياً و مصممي تلك المواقع المعادية قد استغلوا تلك التكنولوجيا لخدمة أغراضهم الشخصية في عرض أفكارهم الشخصية المغرضة التي لم يمتلكوا الشجاعة الكافية في سلك الطرق الشرعية المباحة في عرض تلك الأفكار والآراء .

### و تلك المواقع المعادية قد يكون الغرض منها : -

- ١ - الإساءة إلى دين معين من الأديان و نشر الأفكار السيئة عنه و حث الناس على الابتعاد عنه و تلك المواقع غالباً ما يكون القائمين عليها من معتقي الديانات الأخرى المتشددون في دينهم الذين لا يعتنقون فكرة التسامح و التعايش بين الأديان أو أن يكون هدفهم بث الشقاق فيما بين أفراد الشعب الواحد و المعتنقين لأكثر من دين فيحاولون إثارة الفتنة فيما بينهم عن طريق نشر الأخبار الكاذبة و المضللة في محاولة منهم لتحقيق هدفهم الخبيث .

- ٢ - الإساءة إلى بلد معين و إلى مواقف قادته السياسيين من قضايا الوطن و وهم غالباً ما يكونون من معارضي النظام السياسي القائم في بلد ما فيحاولون نشر الأخبار الفاسدة التي تنشر الفرقة فيما بين أفراد الشعب و نظامه السياسي القائم .

- ٣ - الإساءة إلى شخص معين بما يمثله من مواقف سواء دينية أو سياسية أو وطنية

أو ما إلى ذلك من الأهداف التي لا يجد القائمين عليها من يستمع إلى آرائهم

المغلوبة أو التي تتنافى من الدين و المبادئ و عليه يجد هؤلاء في شبكة الإنترنت ضالتهم المنشودة في الوصول إلى اكبر عدد من الأشخاص لعرض آرائهم عليهم في محاولة منهم لكسب تأييدهم دون تعريف أنفسهم في محاولة منهم للتخفي خوفا من رد فعل الناس التي غالبا ما ترفض مثل تلك الآراء التي بدلا من يجاهر أصحابها بها و اتخاذهم الطريق القانوني الصحيح في نشر أفكارهم و آرائهم ليكون من حق أفراد الطرف الثاني عرض وجهة نظرهم و ردهم على تلك الاتهامات نجد انهم يتخوفون و يتخفون دون أن يمتلكوا أنواع شجاعة في الإعلان عن أنفسهم و في عرضهم لآرائهم .

### التكليف القانوني للجريمة

نقض المواقف السياسية للدولة لمحاولة الوصول إلى السياسة الصحيحة و دون أدنى تعرض للشخصيات و الأعراض هو من الأمور الغير معاقب عليها أما التعرض للشخصيات العامة و انتهاك حرمتهم و التشكيك في أخلاقياتهم فهو من الأمور المجرمة في كافة القوانين .

أما التعرض للأديان فهو من الأمور المجرمة و الغير مقبولة على الإطلاق خاصة في البلاد الإسلامية التي يحث الدين الإسلامي وهو الدين الغالب فيها على احترام الأديان الأخرى و عدم التعرض لمعتقد أي دين اخر .

و في مصر لا تزال القوانين القديمة هي السائدة ولم يتم تعديل أي من قواعد قانون العقوبات ليشمل أي من تلك الجريمتين بطريقة صريحة .

و نحن لا نريد فقط تعديل قانون العقوبات المصري ليشمل تلك الجريمتين بل و لسيجرم بشكل صريح كافة الجرائم الإلكترونية الأخرى دون أن يوضعوا تحت قواعد قديمة لا تتناسب العقوبات المقررة فيها تلك الخسائر و الأضرار التي

تتسبب فيها تلك الجرائم فنحن نريد عقوبات مشددة جدا تتناسب مع ما تسببه تلك الجرائم الإلكترونية الحديثة من أضرار .

## ثامنا : جرائم القرصنة PIRACIES CRIMES

لقد وفرت شبكة الإنترنت في ظل ما توفره من تقنيات حديثة MODERN TECHNIQUES - لكونها تربط العالم اجمع و تلغى الحدود الجغرافية مما أتاح فرصة ارتكاب الجرائم عابرة الحدود CRIMES TRANS BORDER في أوقات قياسية و بأقل قدر من المخاطرة RISKING - مجالا خصبا لنمو نوع جديد من أنواع الجرائم لم يكن معروفا في من قبل ألا وهو الاستخدام غير المشروع - النسخ غير المشروع - لنظم تشغيل و لبرامج الحاسب الآلي COMPUTER .

فمن المعروف أن النسخ غير القانوني لنظم تشغيل و برامج الحاسب الآلي تؤدي إلى خسائر رهيبه لمنتجي تلك البرامج و نظم التشغيل كما أن جرائم القرصنة على البرامج الأصلية ORIGINAL PROGRAMS تؤدي إلى إبطاء عمليات التطور و البحث العلمي لتلك الشركات المنتجة لتلك البرامج نظرا لخسائرها المادية الباهظة نتيجة جرائم القرصنة تلك التي تقع على برامجها التي أنتجتها و أنفقت على تطويرها و إنتاجها الكثير معتمدة على ما ستجنيه من أرباح يعمل على تعويض كل ما أنفقته .

و جرائم القرصنة التي تتم عبر شبكة الإنترنت INTERNET لا تقع فقط على برامج تشغيل الحاسب الآلي COMPUTER و إنما تقع على أي منتجات فكرية أخرى إذ يتم نسخها .

و تشير التقديرات إلى أن هناك حوالي ٣٠٠ مليار صفحة على الأقل يتم إعادة إنتاجها من خلال آلة نسخ واحدة كل سنة على مستوى العالم ويشمل هذا النسخ الصحف والمجلات و النوت الموسيقية ( J.W. Rodlop 99 ) .  
طبعا هذا الرقم يشمل القرصنة ( PIRACIES CRIMES ) التي تتم مقابل الربح المادي و أيضا القرصنة التي تتم و لكن دون أن يكون هدفها تحقيق الربح المادي فالنسخ للاستخدام الداخلي كالمعاهد والجامعات والمدارس والمؤسسات التعليمية والمستشفيات بشكل عام وحتى المنازل يمكن لهم أن ينسخوا لأغراض داخلية وشخصية .

و لم يعد النسخ هذه الأيام مقصورا على آلات التصوير التقليدية فاليوم أصبح النسخ الرقمي الذي يمكن أن يمسح من خلالها ضوئيا ويخزن رقميا باستخدام النسخ عبر الليزر وكذلك الأمر بالنسبة لأسلوب النسخ الألكتروستاتيكي الجاف ( COPYING DRY ELECTROSTATIC ) والذي يمكن أن يستوعب ( ٦٠٠\*٤٠٠ في كل بوصة ) حيث يمكن بعد ذلك بثها في الشبكات وتوسيعها ومسحها ضوئيا وإعادة طباعتها من خلال كمبيوتر وطابعة عادية وقد تكون في بعض الحالات الأعمال المنسوخة أفضل نوعية من الأعمال الأصلية .  
( J.W.RUDOLPH ١٩٩٩ ) .

لقد بات النسخ ( COPY ) بدون إذن أو ترخيص إلى جانب السلبيات والمخاوف التي تخلفها التجارة الإلكترونية يزعج ويقلق مالكي البرامج و منتجيها و الناشرين والمؤلفين وأصبحت التكنولوجيا المتقدمة ومصدر إزعاج لمالكي الحقوق الفكرية والمعنوية مما دعاهم إلى التفكير بتشكيل إدارة جماعية لهذه الحقوق و إحاطة هذه الحماية بأطر قانونية عن طريق المعاهدات الدولية لتتمتع بالحماية القانونية من أجل استغلال هذه الحقوق في عقود الترخيص على غرار عقود الترخيص الخاصة باستعمال علامة تجارية أو



#### استغلال براءة اختراع .

و يتذمر مالكو الحقوق الفكرية والمعنوية ليس فقط من القوانين المحلية والقصور في تطبيقها بل حتى من قصور آليات حسم المعاهدات الدولية حيث أن هذه المعاهدات وتلك القوانين كانت قد وضعت عندما كانت الطباعة تتم بالنسخ باليد أو بالآلة الطباعة العادية وقبل أن يكون هناك آلات تصوير ونسخ بالليزر والتي أصبحت تمكن المستعملين والدارسين من حيازة نسخ الكتب والأبحاث عن طريق تصويرها ونسخها في المكتبات العامة أو الجامعات أو المعاهد أو المدارس أو الشركات لإعادة إنتاج نسخ مجانية لغايات إيضاح التعليم وتسهيله .

هذا من جهة ومن جهة أخرى فإن العولمة التجارية وزيادة استعمال التجار والمستثمرين الشبكات الدولية والبريد الإلكتروني ( E - MAIL ) وتبادل رسائل البيانات إلكترونياً **ELECTRONIC DATA INTERCHANGE ( EDI )** و تحول الكثير من الحكومات إلى ما يسمى بالحكومة الإلكترونية **ELCTRONEC GOVERNMENTS** أدى إلى زيادة اهتمام المجتمع الدولي بالضوابط القانونية للتجارة الإلكترونية **ELECTRONIC COMMERCE** وهذا ما تنبّهت له الجمعية العامة في الأمم المتحدة فوضعت عام ١٩٩٦ قانوناً نموذجياً للتجارة الإلكترونية ( لقانون الأونسترال **UNCTRAL LAW** ) لتقوم الدول الأعضاء بالاسترشاد به .

و قد أدت قرصنة البرامج إلى خسائر مادية باهظة جدا و صلت في عام ١٩٨٨ م إلى حوالي إحدى عشر مليار دولار أمريكي في مجال البرمجيات وحدها و لذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد و إنشاء منظمة خاصة لمراقبة و تحليل سوق البرمجيات و من ذلك منظمة اتحاد

برمجيات الأعمال ( BUSINESS SOFTWARE ALLIANCE ) أو ما يعرف اختصاراً بـ ( B S A ) و التي أجرت دراسة تبين منها أن القرصنة على الإنترنت ستطغى على أنواع القرصنة الأخرى و دق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت في طرح الحلول المختلفة لتفادي القرصنة على الإنترنت و منها تهديد بعض الشركات بفحص القرص الصلب لمتصفحهم مواقعهم على الإنترنت لمعرفة مدى استخدام المتصفح للموقع لبرامج القرصنة إلا أن تلك الشركات قد تراجعت عن هذا التهديد اثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الإنترنت .

### التكليف القانوني للجريمة

تدخل جرائم القرصنة ضمن نطاق جرائم السرقة و عليه فكل القواعد القانونية التي تنطبق على السرقة تنطبق على جرائم القرصنة .

### تاسعا : جرائم التجسس الإلكتروني

## CRIMES OF THE ELECTRONIC ESPIONAGE

عمليات التجسس هي عمليات قديمة قدم البشرية و قدم النزاعات البشرية فمنذ تقدم العصور كان الإنسان يتجسس على أعدائه لمعرفة أخبارهم و الخطط التي يعدونها لمهاجمته و لهذا كان للتجسس أهميته الكبيرة على كافة مستويات النزاعات الإنسانية التي مر بها البشر منذ بدء الخليقة .

و قد تطورت عمليات التجسس طبقا لما يسود المجتمع من تطورات علمية و تكنولوجية .

فمثلا اخترع الإنسان جهاز الرادار ليتجسس على أعدائه و معرفة كافة

تحركاتهم ثم حدث تطور كبير ألا وهو اختراع الأقمار الصناعية التي تقوم بتصوير الإنسان و الآلات الحربية و المدنية و المباني و كل ما هو فوق الأرض يتم تصويره كل فترة زمنية معينة لمعرفة التحركات التي تتم و الآن و في ظل التطور التقني الهائل الذي نعيشه فقد أصبح هناك ما يعرف بالتجسس الإلكتروني .

و التجسس الإلكتروني **ELECTRONIC ESPIONAGE** لا تكمن خطورته إذا ما كان القائم به هم بعض الهواة العابثين **HACKERS** و كان الغرض من اختراقهم لأجهزة الحاسبات الآلية **COMPUTERS** و الشبكات **NETWORK** هو العبث بالمحتويات أو إلغاء **DELETE** بعضها أو كلها إلا أن الأهمية تكمن فيما إذا كان القائم بتلك الاختراقات هي أجهزة المخابرات في بعض الدول للتجسس على الدول الأخرى .

و قد وجدت بعض حالات التجسس الدولي و منها ما اكتشف أخيرا عن مفتاح وكالة الأمن القومي الأمريكية ( **N S A** ) و التي قامت بزراعته في نظام التشغيل الشهير ( ويندوز - **WINDOWS** ) و ربما يكون هذا هو أحد الأسباب الرئيسية التي دعت الحكومة الألمانية بإعلانها في الفترة الأخيرة عن استبدالها لنظام التشغيل ( ويندوز - **WINDOWS** ) بأنظمة تشغيل أخرى .

كما كشف أخيرا النقيب عن شبكة دولية ضخمة للتجسس الإلكتروني **ELECTRONIC ESPIONAGE** تعمل تحت إشراف و وكالة الأمن القومي الأمريكية ( **N S A** ) بالتعاون مع أجهزة الاستخبارات و التجسس في كل من كندا و بريطانيا و نيوزيلندا و يطلق عليها اسم ( **ECHELON** ) لرصد المكالمات الهاتفية و الرسائل بكافة أنواعها سواء ما كان منها برقيا أو تلكس أو فاكس أو إلكترونيا .

و خصص هذا النظام للتعامل مع الأهداف الغير عسكرية و بطريقة تجعله

يعترض كميات هائلة جدا من الاتصالات و الرسائل الإلكترونية عشوائيا باستخدام خاصية الكلمة المفتاح بواسطة الحاسبات المتعددة و التي تم إنشاء العديد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية و منها محطة رصد الأقمار الصناعية الواقعة في منطقة ( واى هوباي ) بجنوب نيوزيلندا و محطة ( جيرالدتون ) الموجودة بأستراليا و كذلك المحطة الموجودة في منطقة ( موروينستو ) بمقاطعة ( كورنوال ) في بريطانيا و المحطة الواقعة في الولايات المتحدة الأمريكية بمنطقة ( شوجر جروف ) وتبعد حوالي مائتي و خمسون كيلو مترا جنوب واشنطن و كذلك المحطة الموجودة بولاية واشنطن على بعد مائتي كيلو مترا جنوب غرب مدينة سياتل .

ولا يقتصر الرصد على المحطات المرتبطة بالأقمار الصناعية و الشبكات الدولية الخاصة بالاتصالات الدولية بل يشمل أيضا رصد الاتصالات الأرضية و كذا الشبكات الإلكترونية أي انه يرصد جميع الاتصالات التي تتم بأي وسيلة و يعتبر الأفراد و المنظمات و الحكومات الذين لا يستخدمون أنظمة الشفرة التأمينية أو أنظمة كودية لحماية شبكاتهم و أجهزتهم أهدافا سهله لشبكة التجسس الإلكتروني **ELECTRONIC ESPIONAGE** هذه و أن كان هذا لا يعنى بالضرورة أن الأهداف الأخرى التي تستخدم أنظمة الشفرة في مامن تام من الغزوات الاستخباراتية لهذه الشبكة و مثيلاتها ولا يقتصر التجسس على المعلومات العسكرية أو السياسية فقط بل تعداه إلى المعلومات التجارية و الاقتصادية بل و حتى الثقافية .

فمع توسع التجارة الإلكترونية **ELECTRONIC COMMERCE** عبر شبكة الإنترنت **INTERNET** تحولت الكثير من مصادر المعلومات إلى أهداف للتجسس التجاري ففي تقرير صدر عن وزارة التجارة و الصناعة البريطانية أشار إلى زيادة نسبة التجسس على الشركات من ( ٣٦ % ) عام



١٩٩٤ م إلى ( ٤٥ % ) عام ١٩٩٩ م كما اظهر استفتاء أجرى عام ١٩٩٦ م لمسئولي الأمن الصناعي في الشركات الأمريكية حصول الكثير من الدول و بشكل غير مشروع على معلومات سرية لأنشطة تجارية و صناعية في الولايات المتحدة الأمريكية .

و من الأساليب الحديثة في التجسس الإلكتروني **ELECTRONIC ESPIONAGE** أسلوب إخفاء المعلومات داخل المعلومات وهو أسلوب شائع و أن كان ليس بالأمر السهل و يتلخص هذا الأسلوب في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة بداخل معلومة أخرى عادية داخل الحاسب الآلي و من ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها و الغير عادية في داخلها و بذلك لا يشك أحد في أن هناك معلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبسا فمن الصعب جدا الوصول إلى تلك المعلومات المغلفة في معلومات أخرى غير مشكوك فيها على الإطلاق .

و من أحدث و أشهر أمثلة التجسس الإلكتروني **ELECTRONIC ESPIONAGE** انه بعد الاعتداءات الأخيرة على الولايات المتحدة الأمريكية في سبتمبر صدرت تعليمات جديدة لأقمار التجسس الأمريكية الصناعية بالتركيز على أفغانستان و البحث عن أسامة بن لادن و الجماعات التابعة و الموالية له و قررت السلطات الأمريكية الاستعانة في عمليات التجسس على أفغانستان بقرنين صناعيين مصممان خصيصا لالتقاط الاتصالات التي تجرى عبر أجهزة اللاسلكي و الهواتف المحمولة بالإضافة إلى قرنين آخرين يلتقطان صورا فائقة الدقة و في نفس الوقت طلب الجيش الأمريكي من شركتين تجاريتين الاستعانة بقرنين تابعين لها لرصد الاتصالات و من ثم تحول بعد ذلك إلى الولايات المتحدة الأمريكية حيث تدخل في أجهزة كومبيوتر **COMPUTER** متطورة لتحليلها .



## التكييف القانوني للجريمة

جرائم التجسس جرائم قديمة و معاقب عليها بأشد العقوبات في كافة القوانين القديمة و الحديثة .

و التجسس الإلكتروني هو أحد أشكال التجسس الحديث كالتجسس بواسطة الأقمار الصناعية و التجسس بواسطة طائرات الاستطلاع المتقدمة إلا انه في معظم الأحيان لا تتمكن الدولة - رغم علمها بأسم الدولة التي تتجسس عليها - من ضبط الشخص الذي يقوم بالتجسس إلا في أحوال معينة وهي إذا ما كان التجسس يتم بالشكل القديم و الذي يتم بأرسال شخص من الدولة إلى الدولة الأخرى للحصول على المعلومات من مصادره في تلك الدولة فيتم التمكن من ضبطه .

## عاشرا : الإرهاب الإلكتروني

### THE ELECTRONIC TERRORISING

في الماضي كان الإرهاب **TERRORISING** يعنى قيام بعض الإرهابيين بتفجير قنبلة في مكان ما أو اغتيال شخصية ما أو تفجير طائرة في الجو و ما إلى ذلك من عمليات روتينية اعتاد رجال الأمن في جميع الدول على مواجهتها و كانت تلك العمليات تتم بغرض نشر الإرهاب في الدولة التي ينتمي إليها الإرهابيين أو حتى في دولة لا ينتمون إليها لتحقيق أغراضهم و التي كان معظمها يتمثل في معارضة النظام الحاكم و ما يمثله من رموز أو تحجيم الحركة السياحية أو اغتيال رموز فكرية تتناقض أفكارها مع فكر الإرهابيين الذين يقومون بتنفيذ تلك العمليات و ما إلى ذلك من أهداف .

أما الآن و مع التقدم التقني **MODERN TECHNIQUES** و مع تقدم

وسائل الاتصالات MODERN COMMUNICATION  
الذي نعيشه و نكاد نلمسه فقد تغيرت و تطورت تلك  
الأساليب SYSTEMS التي يحاول الإرهابيين بها الوصول إلى أهدافهم فقد  
اصبح الإرهاب الإلكتروني هو السائد حاليا و اصبح اقتحام المواقع  
STORMING SITES و تدميرها DISTROYING IT و تغيير  
محتوياتها و الدخول على الشبكات و العبث بمحتوياتها بإزالتها أو بالاستيلاء  
عليها أو الدخول على شبكات الطاقة أو شبكات الاتصالات بهدف تعطيلها عن  
العمل أطول فترة ممكنة أو تدميرها نهائيا اصبح هو أسلوب الإرهاب  
SYSTEMS OF TERRORISING حاليا في محاولة الوصول إلى  
أغراضهم .

و نحن نرى الآن أن الإرهاب TERRORISING الذي تمارسه دولة  
إسرائيل ضد الشعب الفلسطيني PALESTINIAN PEOPLE لا يتمثل فقط  
في اغتيال رموزه بل و أفراد شعبه و تشريد شعبه و استيلاءه على أرضه و  
ممتلكاته و ما إلى ذلك و إنما الإرهاب الذي تمارسه دولة إسرائيل امتد ليشمل  
الإرهاب الإلكتروني فالمواقع الفلسطينية PALESTINIAN SITES  
على شبكة الإنترنت ON THE INTERNET تتعرض و بصفة مستمرة  
من الإسرائيليين إلى الاقتحام و العبث بمحتوياتها و إزالة ما عليها من معلومات  
و عرض صورة العلم الإسرائيلي على الصفحة الرئيسية MAIN PAGE  
بالمواقع المقتحمة THE STORMED SITES و في المقابل يحاول  
الفلسطينيين معالجة تلك الآثار و تصحيح و إزالة العبث الواقع على  
مواقعهم و أيضا يحاولون اقتحام بعض المواقع الإسرائيلية و وضع العلم  
الفلسطيني PALESTINIAN FLAG على الصفحة الرئيسية MAIN  
PAGE بها في المقابل .

و هذا الإرهاب **THISE TERRORISING** لا تقتصر ممارسته على الإسرائيليين الموجودين بإسرائيل فقط و كذلك الفلسطينيين الموجودين بداخل فلسطين فقط و إنما امتد الوضع ليشمل كل من الإسرائيليين و الفلسطينيين الموجودين بالخارج فكل منهم يقوم بمساعدة بلده فاليهود يحاولون مساعدة إسرائيل على استمرار احتلالها لفلسطين و الفلسطينيون يحاولون مساعدة ذويهم بالدخل - داخل فلسطين - في مقاومة الاحتلال **INVASION** الإسرائيلي وقد وفرت لهم شبكة الإنترنت - التي ألغت الحدود الجغرافية بين الدول و - تلك المساعدة التي أصبح في إمكانهم القيام بها من خارج حدود دولتهم - وهو ما ساعد كثيرا الفلسطينيين الموجودين بداخل فلسطين المحتلة فبعد أن كانوا بمفردهم وجها لوجه مع المحتل أصبحوا يجدون المعاونة الخارجية المؤثرة و المفيدة لهم .

### التكليف القانوني للجريمة

كافة بلاد العالم أصبح لديها قوانين خاصة بمكافحة الإرهاب و لكن كل دولة على حدة نظمتها بما يتناسب مع ظروفها الاجتماعية و مع درجة شدة الإرهاب الذي تعانيه .

و كان العالم العربي على قدم المساواة مع العالم الخارجي في تقنين تشريعات جديدة أو تعديل ما لديه من تشريعات ليكون لديه القواعد القانونية الكافية ليحارب الإرهاب الذي يعانيه العالم اجمع إلا أن العالم العربي لما هو معروف عنه السماحة و الخلق القويم لا يعاني من الإرهاب كما يعاني منه العالم الخارجي .

## الفصل الثالث





## مكافحة الجرائم الإلكترونية

### STRIVING THE INTERNET CRIMES

أن مكافحة الجرائم الإلكترونية لن يكون له أي تأثير يذكر إلا إذا كان هناك تعاوناً دولياً على أكبر قدر من التنسيق و التعاون و عليه يمكننا القول أن أي مجهود أو إجراءات قد نقوم بها أي من الدول على مستوى العالم لن يأتي بأي نتائج ملموسة تحد من ارتكاب تلك النوعية من الجرائم فقطلك الجرائم لها طابع خاص تتسم به هو أنها جرائم عابرة للحدود فهي لا تتم من داخل دولة و يكون تأثيرها منحصر في تلك الدولة و إنما تلك الجرائم ترتكب في عبر عدد من الدول لتتم في دول أخرى و تكون أثارها ممتدة لتصل إلى عدد غير محدود من الدول و عليه فأن الأساس الذي يركز عليه مجال مكافحة الجرائم الإلكترونية هو التعاون الدولي و تنسيق الجهود المبذولة بين كافة دول العالم لتكون هناك نتائج مهمة يمكن الارتكاز عليها و تقويتها للحد من تلك الجرائم ذات النتائج البشعة على الاقتصاديات الدول و الكيانات الاقتصادية .

و عليه فسوف يكون تناولنا لمكافحة الجرائم الإلكترونية من خلال التركيز على التعاون الدولي و العناصر التي يركز عليها هذا التعاون و التي تنحصر في الآتي :

- ١ - المعاهدات و المؤتمرات الدولية .
- ٢ - إصدار قوانين جديدة تجرم الجرائم الإلكترونية في كافة أنحاء العالم بحيث يكون بينها قدر كبير من التناسق .
- ٣ - التعاون الدولي .
- ٤ - اتحاد الشركات و الكيانات الاقتصادية الكبرى في مجال حماية أمنها الإلكتروني .

- ٥ - المعاهدات و القوانين الخاصة بحق الملكية الفكرية .

## ١ - المعاهدات و المؤتمرات الدولية

تعد المعاهدات الدولية هي الأساس الذي يركز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية و قد تم عقد العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية و من تلك المعاهدات

### أ - معاهدة بودابست لمكافحة جرائم الإنترنت

## THE BUDAPEST CONVENTION ON CYBER CRIMES

شهدت العاصمة المجرية بودابست في أواخر عام ٢٠٠١ م ميلاد أولى المعاهدات الدولية التي تكافح جرائم الإنترنت INTERNET CRIMES و تسبلور التعاون و التضامن الدولي في محاربتها و محاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص و الممتلكات ،

و يعد التوقيع على تلك المعاهدة دولية - التي تهدف إلى توحيد الجهود الدولية في مجال مكافحة جرائم الإنترنت INTERNET CRIMES و التي انتقلت من مرحلة ابتدائية كانت تتمثل في محاولات التسلل البريئة التي كان يقوم بها هواة في الأغلب الأعم من الحالات و دون أي غرض إجرامي إلى إلى مرحلة جديدة يقوم بها محترفون على أعلى درجة من التخصص و تتمثل في الاحتيال والاختلاس وجرائم تهديد الحياة وهي قضايا تعرض حياة و ممتلكات الكثيرين من رواد شبكة الإنترنت للخطر - هو الخطوة الأولى في

مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم على شبكة الإنترنت و استخدامها الاستخدام الأسوأ .

و يعد التوقيع على تلك الاتفاقية - من المسؤولين في الدول الأوروبية إضافة إلى أمريكا و اليابان و كندا و جنوب أفريقيا - هو نتاج مباحثات و مفاوضات استغرقت أكثر من أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الاتفاقية حتى يتم التوقيع عليها من جميع الأطراف دون أن تجد أي اعتراض من أي منهم بل على العكس لتجد القبول من أطراف جدد ليتم توسيع دائرة الدول التي توافق على الانضمام إلى تلك الاتفاقية و يتم توسيع الاتحاد الدولي و التضامن الدولي في مجال مكافحة جرائم الإنترنت INTERNET  
• CRIMES

و قد أجريت العديد من الدراسات على مجال التضامن الدولي في مكافحة جرائم الإنترنت أوضحت أن العديد من الدول لا تستطيع بمفردها مواجهة تلك الجرائم التي ترتكب عبر الإنترنت مهما سنت من قوانين و مهما غلظت من عقوبات تلك الجرائم نظرا لكون تلك الجرائم هي من الجرائم عابرة الحدود CRIMES TRANS BOEDER التي لا يقف أمامها أي عائق جغرافي و بالتالي فتلك الدول تفضل الانضمام إلى المعاهدات الدولية التي تبرم في هذا المجال نظرا لكبر حجم الأضرار التي تصيبها سواء المادية أو لكثرة الجرائم الأخلاقية التي يتم ارتكابها عن طريق الإنترنت ولأن العديد من الدول حتى المتقدمة منها لا تستطيع مواجهة تلك الأخطار بمفردها دون وجود تعاون و تضامن دولي ليتم نجاح أي مجهودات تبذل في مجال مكافحة الجرائم التي ترتكب عبر الإنترنت  
• INTERNET CRIMES

وقد ذكرت إحدى الدراسات حادثة كمثال عما يمكن أن تحدثه جريمة تتم عبر الإنترنت عندما سيطر أحدهم على نظام الكمبيوتر الخاص بمطار أمريكي و قام بإطفاء مصابيح الإضاءة الموجودة على ممرات الهبوط و وهو أمر يمكن أن يؤدي إلى سقوط الطائرات و وفاة الكثير من الأشخاص و بعد أن تم التكهّن بأن وراء الحادث عمل إرهابي تم اكتشاف أن وراءه مراقب من كاليفورنيا و عليه فالتعاون الدولي أمر هام جدا في مجال مكافحة تلك الجرائم ففي مثل تلك الحالات يتسلل الجاني عبر العديد من الدول قبل أن يصل إلى نظام الكمبيوتر هذا .

وعليه فإن التعاون و التضامن الدولي أمر هام جدا في مجال مكافحة جرائم الإنترنت و بدون هذا التعاون الدولي لن يكون هناك أي اثر لأي مجهود تقوم به أي من الدول بمفردها نظرا لأنه سيكون عديم الفائدة و بلا اثر تقريبا و لن يؤدي إلى الحد من ارتكاب تلك الجرائم التي تكون في الأغلب الأعم من الحالات جرائم عابرة للحدود **CRIMES TRANS BOEDER** .

هذا من جهة و من جهة أخرى فحتى الجرائم التقليدية التي تتم عبر الإنترنت مثل النصب و الاحتيال و الاختلاس و انتهاك حقوق الملكية الفكرية فهي أيضا من الجرائم التي لا يمكن مواجهتها بصفة فردية كل دولة على حدة بل أن تلك الجرائم أيضا تحتاج إلى التعاون الدولي ليكون في الإمكان مكافحتها و مواجهتها و محاولة الحد من ارتكابها و ملاحقة مرتكبيها و ضبطهم لينالوا العقاب **PUNISHMENT** على ما اقترفت أيديهم فوضع قوانين تحمي الملكية الفكرية في كل دولة على حدة لا يكفي بأي حال من الأحوال للمحافظة على تلك الحقوق و إنما التعاون الدولي في تطبيق تلك القوانين هو الطريق الوحيد ليتم احترام مثل تلك الحقوق التي تجد دائما من ينتهكها أو على الأقل من يحاول



انتهاكها .

و قد كان الخلاف الوحيد فيما بين الدول الموقعة على الاتفاقية هو مجال محاربة العنصرية فالدول الأوروبية تعتبر أن التحريض على الكراهية العنصرية هي جريمة **INCITATION TO THE RACIALIST HATING IS A CRIME** و من المعروف أن هذه الجريمة يعاقب عليها القانون الدولي **THIS CRIME IS PUNISHING BY THE INTERNATIONAL LAW** و بالتالي فلا بد من النص في الاتفاقية على لزوم العمل على إزالة تلك المواقع التي تعمل على التحريض على الكراهية العنصرية **INCITATION TO THE RACIALIST HATING** و مسألة القائمين عليها على أساس أنهم يرتكبون جريمة يعاقب عليها القانون الأوروبي بينما الولايات المتحدة الأمريكية تعتبر أن حرية التعبير المنصوص عليها في الدستور الأمريكي تتعارض مع ما تراه الدول الأوروبية من أن التحريض على الكراهية العنصرية جريمة يعاقب عليها القانون و بالتالي فهي ترى أنه لا مجال للنص في الاتفاقية على العمل على إزالة تلك المواقع **SITES** على أساس أن الدستور الأمريكي لا يري في تلك المواقع أي جريمة بل أنها تقوم بالتعبير عن رأيها و هو ما كفله الدستور الأمريكي إلا أنه تم الاتفاق فيما بين الجميع على عدم تضمين الاتفاقية ذلك الموضوع على أساس تقليل حدة الخلاف فيما بين الدول الأعضاء الموقعة على الاتفاقية و ذلك إلى أن يتم دراسة الموضوع من كافة الاتجاهات و محاولة الوصول إلى نقطة وسط يتلاقى عندها كافة الأطراف .

ومن ضمن الجوانب العديدة التي تناولتها تلك الاتفاقية الإرهاب الإلكتروني و عمليات تزوير بطاقات الائتمان و دعارة الأطفال و تلك الجرائم تعتبر من أكثر



الجرائم انتشارا على المستوى العالمية بصفة عامة و في أوروبا و أمريكا بصفة خاصة و لم تفلح أي جهود فردية تم بذلها من جانب أي من الدول الموقعة على الاتفاقية و عليه فقد كان من المحتم التنسيق بين تلك الجهود على اقل تقدير أن لم يكن التوحيد بينها لتؤتى ثمارها في الحد من ارتكاب تلك الجرائم التي تؤثر على التقدم الاقتصادي الذي المتواصل في اقتصاديات تلك الدول المتقدمة .

وقد صاغ نصها عدد من الخبراء القانونيين في مجلس أوروبا بمساعدة دول أخرى وبالأخص الولايات المتحدة .

وتحدد الاتفاقية أفضل الطرق الواجب إتباعها في التحقيق في جرائم الإنترنت **INTERNET CRIMES** التي تعهدت الدول الموقعة بالتعاون الوثيق من أجل محاربتها كما تحاول إقامة توازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة والقلق الذي عبرت عنه المنظمات المدافعة عن حقوق الإنسان **HUMAN RIGHTS** والصناعات المعنية ومزودي خدمات الإنترنت .

وتخشى منظمات حقوق الإنسان من أن تحد الاتفاقية من حرية الأفراد في أعقاب الهجمات على الولايات المتحدة

كما أن القلق يتزايد من أن تؤدي زيادة الرقابة إلى انتهاك حقوق مستخدمي الإنترنت .

وهو ما يتعارض مع الإعلان العالمي لحقوق الإنسان **HUMAN RIGHTS** الصادر من الأمم المتحدة و الذي ينص في المادة الثانية عشر منه على انه لا يتعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته .

كما أن المادة التاسعة عشر من هذا الإعلان تنص على انه لكل شخص الحق

في حرية الرأي و التعبير و يشمل هذا الحق حرية اعتناق الآراء دون أي تدخل و استقاء الأنباء و الأفكار و تلقيها و إذاعتها بأي وسيلة كانت دون تقيد بالحدود الجغرافية .

إلا أن تلك الحقوق التي نص عليها الإعلان العالمية لحقوق الإنسان الصادر من هيئة الأمم المتحدة لم يترك تلك الحقوق الإنسانية لتمارس دون أي قيود إذ أنه قد نص في المادة التاسعة و العشرين على أنه ( يخضع الفرد في ممارسة حقوقه و حرياته إلى تلك القيود التي يقرها القانون فقط لضمان الاعتراف بحقوق الغير و حرياته و احترامها و لتحقيق المقتضيات العادلة للنظام العام و المصلحة العامة و الأخلاق في مجتمع ديمقراطي .

و عليه فنحن نرى أن تلك المعاهدة التي لا غرض لها إلا احترام حقوق الإنسان HUMAN RIGHTS و الحد من تعرضه للكم الهائل من الجرائم التي ترتكب عبر شبكة الإنترنت لا تتعارض بأي حال من الأحوال مع الإعلان العالمي لحقوق الإنسان الذي يعد الأساس في تقرير حريات الأشخاص .

## ب - المعاهدة الأوروبية لمكافحة جرائم الإنترنت

وقعت اللجنة الخاصة المعنية بقضايا الجريمة بتكليف من المجلس الأوروبي على المسودة النهائية لمعاهدة شاملة تهدف لمساعدة البلدان في مكافحة جرائم الإنترنت وسط انتقادات من دعاة حماية الحرية الشخصية وبعد أن يتم المصادقة عليها من قبل رئاسة المجلس وتوقيعها من قبل البلدان المعنية ستلزم الاتفاقية الدول الموقعة عليها بسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية بما في ذلك الدخول غير المصرح به إلى شبكة ما والتلاعب

بالبيانات وجرائم الاحتيال والتزوير التي لها صلة بالكمبيوتر وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي .

وتتضمن بنود المعاهدة التي تم تعديل مسودتها ٢٧ مرة قبل الموافقة عليها فقرات تكفل للحكومات حق المراقبة وتلزم الدول بمساعدة بعضها في جمع الأدلة وفرض القانون لكن الصلاحيات الدولية الجديدة ستكون على حساب حماية المواطنين من إساءة الحكومات استخدام السلطات التي أعطتها لهم تلك الاتفاقية التي قد يستخدمونها

٢ - إصدار قوانين جديدة تجرم الجرائم الإلكترونية في كافة أنحاء العالم بحيث يكون بينها قدر كبير من التناسق

اتجهت كافة الدول المتقدمة تكنولوجيا إلى استحداث نصوص قانونية جديدة تجرم تلك الجرائم الإلكترونية **MADE A NEW LAWS FOR THE ELECTRONIC CRIMES** الجديدة على قوانينها التقليدية القديمة و عليه فقد صاغت تلك الدول نصوص قانونية جديدة قادرة على التعامل مع تلك الجرائم الجديدة و المتطورة تكنولوجيا .

أ - على المستوى العالمي

تعتبر دولة السويد من أوائل الدول التي اتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الإنترنت **MADE A NEW LAWS FOR THE INTERNET CRIMES AND COMPUTERS CRIMES** و الحاسب الآلى لتمتطيح أن تعاقب المتهمين بأرتكاب تلك الجرائم الإلكترونية

## TO CAN PUNISH THE DEFENDANTS WITH حيث PERPETRATING THE ELECTRONIC CRIMES

صدر أول قانون خاص بها 'THE FIRST SPECIAL LAW' سمي  
بقانون ( البيانات ) و قد صدر هذا القانون عام ١٩٧٢ م و قد عالج هذا  
القانون قضايا الاحتيال عن طريق الإنترنت بالإضافة إلى كونه يشتمل على  
فقرات عامة من نصوصه لتشمل جرائم الدخول غير المشروع على البيانات  
الإلكترونية THE UNLEGAL ENTERING TO THE  
ELECTRONIC INFORMATION أو تزوير المعلومات الإلكترونية  
FORGING THE ELECTRONIC INFORMATION أو  
تحويلها أو الحصول غير المشروع عليها .

و كانت الولايات المتحدة الأمريكية هي الدولة التالية التي تبعت السويد في  
إصدار قوانين خاصة بها SPECIAL LAWS تجرم الجرائم الإلكترونية  
حيث شرعت قانونا خاصا SPECIAL LAW بحماية أنظمة الحاسب  
الآلي ( ١٩٧٦ م - ١٩٨٥ م ) و في عام ١٩٨٥ م حدد معهد العدالة القومي  
الأمريكي خمسة أنواع رئيسية للجرائم المعلوماتية و هي :

- جرائم الحاسب الآلي الداخلية
  - جرائم الاستخدام غير المشروع عن بعد
  - جرائم التلاعب بالحاسب الآلي
  - دعم التعاملات الإجرامية
  - سرقة البرامج الجاهزة و المكونات المادية للحاسب
- و في عام ١٩٨٦ م صدر قانونا آخر يحمل الرقم ١٢١٣ عرف كافة  
المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت  
المتطلبات الضرورية اللازمة لتطبيقه .

و على اثر ذلك قامت الولايات الداخلية بإصدار التشريعات الخاصة بكل منها على حده للتعامل بها مع تلك الجرائم الإلكترونية **ELECTRONIC CRIMES** و من تلك القوانين القانون الخاص بولاية تكساس لجرائم الحاسب الآلي .

و قد خولت وزارة العدل الأمريكية في عام ٢٠٠٠ م خمس جهات حكومية للتعامل مع جرائم الإنترنت و الحاسب الآلي منها مكتب التحقيقات الفيدرالي **FBI** .

أما بريطانيا فهي ثالث دولة تسن قانون خاص بها **SPECIAL LAW** بجرائم الإنترنت حيث أقرت قانون لمكافحة التزوير و التزييف عام ١٩٨١ م الذي شمل في تعاريفه الخاصة تعريف أداة التزوير **DEFINITION OF FACILITY OF THE FORGING** و وسائط التخزين الحاسوبية المتسوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق الإلكترونية أو التقليدية أو أي طرق أخرى .

أما كندا فهي تطبق قوانين متخصصة و مفصلة للتعامل مع جرائم الإنترنت **INTERNET CRIMES** حيث عدلت في عام ١٩٨٥ م قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي و الإنترنت كما شمل القانون الجديد أيضا تحديد للعقوبات المطبقة على المخالفات الحاسوبية و جرائم التدمير و جرائم الدخول غير المشروع على المعلومات الإلكترونية **THE UNLEGAL ENTERING TO THE ELECTRONIC INFORMATION** كما وضع القانون صلاحيات جهات التحقيق كما جاء في قانون المنافسة الذي يخول لمأموري التبض القضائي متى حصل على أمر قضائي حق التفتيش على أنظمة الحاسب الآلي و التعامل معها و ضبطها .

أما الدانمارك فقد انتهت لائحة الأمر مبكرا أيضا فقد سنت أول قانون الخاص



**THE FIRST SPECIAL LAW STRIVING THE INTERNET CRIMES AND THE COMPUTERS CRIMES** و الحاسب الآلي في عام ١٩٨٥ م و قد شمل القانون العقوبات المحددة على ما يرتكب من جرائم مثل الدخول غير المشروع إلى الحاسب الآلي **THE UNLEGAL ENTERING TO FORGING THE THE COMPUTERS ELECTRONIC DATA** سواء كان هذا التزوير بالحذف أو بالإضافة أو بالتعديل .

أما فرنسا فهي من الدول التي اهتمت بتطوير القوانين الخاصة بها للتوائم مع الجرائم التكنولوجية الحديثة - جرائم الإنترنت **INTERNET CRIMES** - فقد طورت فرنسا قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت أول قانون خاص بها **THE FIRST SPECIAL LAW** في عام ١٩٨٨ م القانون رقم ( ١٩ - ٨٨ ) و الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي و العقوبات المقررة لتلك الجرائم كما تم في عام ١٩٩٤ م تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية و قد أوكل هذا القانون **LAW** إلى النيابة العامة سلطة التحقيق فيها بما في ذلك طلب عمل التحريات و سماع الأقوال و الشهود .

أما هولندا فقد قامت هي أخرى بتعديل القوانين الخاصة بها للتوائم مع تلك الجرائم الحديثة ليكون في إمكانها التعامل معها و محاولة السيطرة عليها فقد قامت بتعديل القوانين الخاصة بها و نصت في تلك القوانين على انه من حق القاضي أن يصدر أوامره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة و متى كان هذا التصنت على قدر عال من الأهمية للكشف

عن تلك الجريمة .

أما فنلندا فهي الأخرى قد قامت بتعديل قوانينها الجنائية لتتسع لتلك الجرائم الإلكترونية الحديثة **THE MODERN ELECTRONIC CRIMES** و طبقا لتلك التعديلات فقد أصبح لمأمور الضبط القضائي الحق في التصنت على المكالمات الخاصة بشبكات الحاسب الآلي .

أما في ألمانيا فقد تم تعديل القوانين الخاصة بها و أصبح للقاضي الحق في إصدار أوامره بمراقبة اتصالات الحاسب الآلي و تسجيلها و التعامل معها إلا أن القانون قد أعطى ذلك المحقق بشرط إلا في مدة أقصاها ثلاثة أيام .

أما في اليابان فقد قامت هي الأخرى بسن القوانين الخاصة بها لتستوعب المستجدات الإجرامية المتمثلة في جرائم الإنترنت و الحاسب الآلي و قد نصت تلك القوانين على انه لا يلزم مالك الحاسب الآلي **OWNER OF THE COMPUTER** المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمة السر **DIVULGING THE PASSWORD** التي يستخدمها إذا ما كان ذلك سيؤدي إلى أدانته كما أقرت في قانون خاص **SPECIAL LAW** سنته عام ١٩٩١ م شرعية التصنت على شبكات الحاسب الآلي فقط إذا ما كان ذلك في مجال البحث عن الأدلة الخاصة بإحدى الجرائم الإلكترونية

• **THE EVIDENCE OF THE INTERNET CRIME**

وفي دولة المجر فقد قامت هي أخرى بسن قوانين خاصة بها لتجرم الجرائم الإلكترونية **INTERNET CRIMES** و قد نصت تلك القوانين التي سنتها على كيفية التعامل مع مثل هذا النوع من الجرائم و أيضا كيفية التعامل مع المتهمين بارتكاب الجرائم **DEFENDANTS WITH PERPETRATING THE CRIMES** و هي الإجراءات التي تسهل عمل الجهات المنوط بها مواجهة مثل تلك الجرائم و القبض على المتهمين

بارتكابها .

أما في دولة بولندا فهي أيضا سنت القوانين الخاصة بها و تلك القوانين التي سنتها تنص على أن للمتهم بارتكاب الجرائم **DEFENDANT WITH PERPETRATING THE CRIMES** الحق في عدم طبع أي سجلات خاصة بالحاسب الآلي أو إفشاء كلمات السر المستخدمة أو حتى ألا كواد الخاصة بالبرامج كما أنها تنص على حقوق أخرى بالنسبة للشهود **WITNESSES** في تلك الجرائم فهي تعطي الشاهد **WITNESS** أيضا الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى كان ذلك قد يؤدي إلى أدانته أو إدانة أي من أقاربه بل أن تلك القوانين تذهب إلى مدى أبعد من ذلك فتلك القوانين تنص على أن لا يقابل ذلك أي إجراء قسري قد يتخذ و تكون من نتائج إدانة بالمتهم **CONDEMNING THE DEFENDANT**

١

ب - على المستوى العربي

أما عن الحال في الدول العربية فانه للأسف لا توجد أي دولة عربية قد قامت بسن قوانين جديدة **NEW LAWS** خاصة بها أو حتى تحديث قوانينها **MODERNISATION THE LAW** الخاصة لتستوعب تلك المستجدات الإجرامية فالدول العربية لا زالت بعيدة كل البعد عن ذلك التطور القانوني **EVOLUTION OF LAWS** الذي يحاول اللحاق بالتطور الإجرامي بينما نجد أن الدول العربية لا زالت لا تحرك ساكنا .  
فمصر على سبيل المثال لا الحصر لم تعمل على سن قوانين جديدة خاصة بها في هذا المجال و لم تقم حتى بتعديل ما لديها من قوانين و إنما القانونيين في

مصر يحاولون تطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية و التي تفرض نوعا من الحماية الجنائية ضد الأفعال المشابهة بالأفعال المكونة لأركان الجريمة المعلوماتية و من ذلك على سبيل المثال اعتبر أن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات كما تم تطويع نصوص قانون حماية الحياة الخاصة و قانون تجريم إفشاء الأسرار بحيث يمكن تطبيقها على بعض جرائم الإنترنت INTERNET CRIMES و أوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية .

و عليه فإن وجد نص قانوني يعاقب على جريمة شبيهة بالجريمة المعلوماتية يتم إدراجها تحته و تتقرر العقوبة المنصوص عليها في ذلك النص و عليه و دائما و في جميع الأحوال لا تكون العقوبة المنصوص عليها في هذا النص القانوني متناسب و حجم الخسائر الناتجة عن ارتكاب مثل تلك الجريمة الإلكترونية و لأنه لا يوجد نص صريح CANDID TEXT خاص بها و يعاقب عليها و يعطى العقوبة المناسبة للأضرار الناتجة من تلك الجريمة يتم إدراج تلك الجريمة المعلوماتية تحت هذا النص القانوني LAW TEXT الغير خاص بها و الموضوع للعقاب على جريمة أخرى و بالتالي لا يكون العقاب المنصوص عليه مناسب .

أما في المملكة العربية السعودية فهي لا تواجه نفس تلك المشاكل على أساس أن كافة تشريعاتها LAWS تنطلق من الشريعة الإسلامية و بالتالي فهي لا تحتاج إلى تحديث فالشريعة الإسلامية لا تحتاج إلى أي تحديث فالشريعة الإسلامية صالحة لكل زمان و مكان .

وقد اتخذت مدينة الملك عبد العزيز للعلوم و التقنية من خلال وحدة الإنترنت المشرفة على عمل مقدمي خدمة الإنترنت INTERNET في المملكة عدد



من الإجراءات الفنية التي تهدف إلى محاصرة أعمال المخربين و المتسللين و منعهم و قد أوضحت الوحدة أنها قد ألزمت جميع مقدمي خدمة الإنترنت في المملكة بتطبيق عدد من الإجراءات الفنية لمنع أعمال المتسللين و إساءة استخدام البريد الإلكتروني E \_ MAIL و غيرها من المخالفات المتوقعة بالجوانب الأمنية لاستخدام شبكة الإنترنت في المملكة و من بين هذه الإجراءات ما يأتي :

- ١ - منع انتحال أرقام الإنترنت أو ما يعرف بـ ( IP - SPOOFING ) و التي يقوم من خلالها بعض المتسللين المحترفين باستخدام أرقام بعض الأشخاص بطريقة غير مشروعة .
- ٢ - العمل على منع إساءة استعمال البريد الإلكتروني أو ما يعرف بـ ( E \_ MAIL SPAMMING ) سواء للتهديد أو لإرسال عروض أسعار أو دعايات لا يقبل بها المستخدم وهو ما عرف اصطلاحاً بأسم البريد المهمل و الذي ينتشر بشكل كبير في الدول المتقدمة .
- ٣ - DIALUP - SERVER أي الاحتفاظ بسجل استخدام مزود الاتصال الخاص بالمستخدمين و سجل استخدام البروكسي PROXY لمدة لا تقل عن ستة أشهر .
- ٤ - الحصول على خدمة الوقت LTP عن طريق وحدة البروكسي و مزود الاتصال بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات .
- ٥ - تحديث سجلات منظمة رايب WWW . RIPE . COM الخاصة بمقدمة الخدمة .
- ٦ - ضرورة تنفيذ ما تتوصل إليه اللجنة الأمنية الدائمة بخصوص متابعة و معاقبة المخالفات الأمنية .



### ٣ - التعاون الدولي

من المعروف أن جرائم الإنترنت هي جرائم عابرة للحدود أي أنها لا تتم و تنتهي في أراضي دولة بعينها و عليه فالتعاون الدولي هو من أهم سبل مكافحة جرائم الإنترنت و ملاحقة مرتكبيها فبغير التعاون الدولي يزداد معدل ارتكاب تلك الجرائم و يطمئن مرتكبوها من عدم إمكانية ملاحقتهم إذ يكون من السهل عليهم التنقل من دولة إلى أخرى تبيح القوانين السارية بها ما ارتكبه من جرائم .

و تعتبر المعاهدات الدولية التي تنضم إليها العديد من الدول هي النموذج الذي يكون هذا التعاون الدولي في ذلك المجال .

و مثال ذلك أيضا التعاون الدولي في مجال مكافحة الجريمة المنظمة و قد بدأ هذا التعاون الدولي بمؤتمر الأمم المتحدة السابع و الذي عقد عام ١٩٨٥ م لمنع الجريمة المنظمة حيث اعتمد خطة عمل ميلانو و التي أوصت بعدة توصيات حيال التعامل مع الجريمة المنظمة و القضاء عليها .

و تبع ذلك الاجتماع الإقليمي التحضيري و الذي عقد عام ١٩٨٨ م و الذي تم فيه إقرار المبادئ التوجيهية لمنع الجريمة المنظمة و مكافحتها ثم المؤتمر الثامن لمنع الجريمة بفنزويلا عام ١٩٩٠ م فالمؤتمر الوزاري العالمي المعنى بالجريمة المنظمة عبر الوطنية في نابولي بإيطاليا عام ١٩٩٤ م و الذي عبر عن إرادة المجتمع الدولي بتعزيز التعاون الدولي و إعطاؤه الأولوية لمكافحة الجريمة المنظمة .

و كانت معاهدة المجلس الأوروبي حول جرائم الشبكات الإلكترونية التي أيدتها الولايات المتحدة بقوة هي أول خطوة رئيسية في هذا الاتجاه ويمكن اعتبارها بداية لعملية وضع القواعد والمعايير التي يتوقع من البلدان المعنية أن تتبعها

في نهاية الأمر في جهودها التشريعية والتنظيمية وتطبيق القوانين .

و يستند نهج هذه المعاهدة إلى اعتراف أساسي بضرورة قيام انسجام بين قوانين الدول المعنية و قد تم تحقيق التعاون الدولي في تطبيق القوانين من خلال سلسلة من معاهدات تسليم المجرمين والمساعدة القانونية المتبادلة (MLAT) التي تمكن الحكومات من تبادل المعلومات والأدلة وبغية وضع هذه المعاهدات قيد التنفيذ يفترض عادة وجود ما يعرف بازدواج العمل الإجرامي ( أي ان تكون السلطات القضائية لكلا الدولتين تعتبر ذلك العمل عملاً جرمياً ) و عليه يتم تسهيل التعاون الدولي بدرجة كبيرة من خلال التلاقي على ما يمكن اعتباره عملاً إجرامياً بموجب تشريعات مختلف البلدان المعنية فان فرض قوانين مماثلة في مختلف الدول يزيد المخاطر التي تواجه مرتكبي جرائم الإنترنت وبتجه أكثر نحو معادلة هذه المخاطر في مختلف الدول المعنية وفي الواقع كلما كانت القوانين أكثر شمولاً كلما قلت الملاذات الآمنة التي يستطيع المعتقدون على الشبكات الإلكترونية العمل انطلاقاً منها بأمان .

ان الانسجام ضروري بالنسبة إلى القوانين الأساسية كما بالنسبة إلى القوانين الإجرائية و على كافة الدول ان تعيد تقييم ومراجعة قواعد الإثبات و التفتيش وإلقاء القبض والتنصت الإلكتروني وما شابه ذلك لتشمل المعلومات الرقمية وأنظمة الكمبيوتر الحديثة وأنظمة الاتصالات الحديثة والطبيعة العالمية لشبكة الإنترنت أما التنسيق الأكبر للقوانين الإجرائية فيمكن أن يُسهل التعاون في التحقيقات التي تشمل سلطات قطاعية متعددة .

بالإضافة إلى القوانين الملائمة من المهم أيضاً ان تطور الحكومات وأجهزة تطبيق القانون قدراتها على تطبيق هذه القوانين يحتاج ذلك إلى تطوير الخبرات في مجال الجريمة التي ترتكب عبر الشبكات الإلكترونية وتحقيق مشاركة فعالة

للمعلومات بين الدوائر داخل الدولة المعنية وبين مختلف الدول يضاف إلى ذلك ضرورة تخطي هذه المشاركة الأجهزة التقليدية لتطبيق القوانين بحيث تشمل أجهزة الأمن القومي وأجهزة الاستخبارات كما أن من الأمور الأساسية تشكيل وحدات متخصصة في تطبيق القانون للتعامل مع المسائل المتعلقة بهذا النوع من الجرائم على مستوى البلد المعني بإمكان هذه الوحدات أيضاً أن توفر أساساً للتعاون الدولي الرسمي وغير الرسمي المستند إلى شبكات ثقة بين مسؤولي تطبيق القوانين في مختلف البلدان ويمكن للتعاون في قضية معينة أو التعاون في لجان مشتركة مؤلفة من ممثلي عدد من الدول أن يكون مفيداً جداً وهناك قضايا كان فيها التعاون الدولي فعالاً للغاية وبالفعل يمكن أن يولد التعاون الناجح تعاوناً مماثلاً في أماكن أخرى ويحقق المزيد من النجاح .

و على مستوى العالم العربي وضعت لجنة مكافحة الجرائم المنظمة مقترحات للعمل العربي في مكافحة الإرهاب و التي وافق عليها مجلس وزراء الداخلية العرب في دورته السادسة و في عام ١٩٩٦ م وافق المجلس في دورته الثالثة عشر على مدونة سلوك طوعية لمكافحة الإرهاب ووافق عام ١٩٩٧ م في دورته الرابعة عشر على استراتيجية عربية لمكافحة إرهاب وفي عام ١٩٩٨ م أقر مجلس وزراء الداخلية و العدل العرب الاتفاقية العربية لمكافحة الإرهاب .

هذا في مجال مكافحة الجرائم المنظمة أما في مجال التعاون الدولي لمكافحة الاتجار في المخدرات فقد اهتمت كافة الدول بهذا الموضوع لما يسببه من أضرار على اقتصادياتها و كذلك لما يسببه من انتهاك لثروتها البشرية و التي تعتمد عليها أي دولي في تحقيق تقدمها الاقتصادي و عليه فقد كان هناك تعاوناً دولياً قوياً في مجال مكافحة الاتجار في المخدرات و مساعدة المدمنين على الإقلاع عن الإدمان .

وقد عقدت اتفاقية مكافحة المخدرات عام ١٩٦١ م و اتفاقية المؤثرات العقلية عام ١٩٧١ م و اتفاقية الأمم المتحدة لمكافحة الاتجار في المخدرات و المؤثرات العقلية عام ١٩٨٨ م .

و على المستوى العربي تم عام ١٩٩٦ م إقرار الاتفاقية العربية لمكافحة الاتجار في المخدرات و المؤثرات العقلية كما تم في عام ١٩٩٦ م إقرار القانون العربي النموذجي الموحد للمخدرات

و عليه فإنه لتفعيل التعاون الدولي لابد من التركيز على ثلاث موضوعات رئيسية لابد من العمل على تعظيم وجودها و الأخذ بها وهي كآلاتي : -

- ١ - الانضمام إلى المعاهدات الدولية التي تعمل على زيادة التعاون و التنسيق بين الجهود التي تبذلها الدول في مجال مكافحة جرائم الإنترنت

- ٢ - إدخال تلك المعاهدات الدولية إلى حيز التنفيذ الفعلي أي تنفيذ ما تنص عليه تلك الاتفاقيات من إجراءات دون أي إبطاء

- ٣ - العمل على وجود اكبر قدر ممكن من التناسق و التطابق فيما بين قوانين الدول المختلفة و المنطقة بمكافحة جرائم الإنترنت فلا يكون الفعل الذي تم ارتكابه جريمة في بلد ما و غير معاقب عليه في قانون بلد آخر فمن هنا يجد المجرمون الملاذ الأمن الذي يلجئون إليه دون أي اعتبار لما ارتكبوه من جرائم .

- ٤ - تعاون جميع الدول في تسليم المطلوبين أمنيا إلى الدول التي تطالب بهم لارتكابهم جرائم الإنترنت .



## ٤ - اتحاد الشركات و الكيانات الاقتصادية في مجال حماية أمنها الإلكتروني

تعد الكيانات الاقتصادية من أهم الأهداف المحتملة لأي عمليات إجرامية تتم عبر الإنترنت و غالبا ما يكون الهدف من ارتكاب تلك الجرائم هو البحث عن أموال تلك الشركات الضخمة أو عما تخفيه من معلومات تريد الشركات الأخرى الحصول عليها في محاولة منها للتغلب على ما تعانيه من نقص في المعلومات التكنولوجية التي تساعد على النهوض تكنولوجيا و تصبح في عداد الشركات الاقتصادية الكبرى و المتقدمة اقتصاديا بما يعود عليها من فوائد اقتصادية ضخمة و عليه فغالبا ما تكون الشركات الاقتصادية هي الهدف السمين الذي يلهث وراءه مرتكبي جرائم الإنترنت .

أيضا قد يكون الهدف من الجرائم التي تتعرض لها تلك الشركات الاقتصادية الضخمة هي الحصول على معلومات هامة عنها للقيام بابتزازها و الحصول منها على مبالغ مالية في مقابل عدم نشر ما تم الاستيلاء عليه من معلومات في الغالب يكون نشرها ضارا بالشركة ضرا بالغا .

و عليه فأن الكثير من الكيانات الاقتصادية الهامة في العالم تتحد مع بعضها البعض في محاولة منها للقيام ببناء حائط صد إلكتروني مضاد لما قد تتعرض له من هجمات و محاولات اختراق و قرصنة من محترفي ارتكاب جرائم الإنترنت و مكاسب تلك الكيانات الاقتصادية عظيمة من تعاونها مع بعضها البعض في هذا الأمر .

- ١ - فمن ناحية فأن التعاون الذي يتم بينها و بين الكيانات الاقتصادية

الأخرى يوفر لها قدرا كبيرا من الأموال فيما لو كانت ستقوم ببناء هذا



- الحائط المضاد بمفردها فعندها كانت ستتحمّل بمفردها ما يتكلّفه من أموال دون أي مساعدة من أي جهة خارجية

- ٢ - و من ناحية أخرى فإن هذا الاتحاد يكون ائتلافا قويا في مواجهة تلك الهجمات التتارية على تلك الكيانات و بالتالي يجعلها أقوى عند مواجهة تلك الاختراقات و صدها و تعقب مرتكبيها .

- ٣ - أن تعاون تلك الشركات و عدم تحمّل أي منها للتكاليف بمفرده يجعلها تستطيع القيام ببناء حائط صد قوى و منيع في مواجهة مرتكبي جرائم الإنترنت و بالتالي يصعب كثيرا من فرص اختراقه و النفاذ إلى تلك الشركات .

و عليه نجد أن تعاون الكيانات الاقتصادية الكبرى في مجال مكافحة جرائم الإنترنت يساعد كثيرا على حماية امنها من مخاطر التعرض لتلك الجرائم و يحافظ عليها من أي محاولات ابتزاز قد تتعرض لها إذا ما استطاع أي شخص السنفاذ إلى معلوماتها و الحصول عليها فعندئذ سيكون عليها أن تدفع له الكثير من الأموال لمنعه من نشر معلوماتها السرية و التي قد تستفيد منها أي شركات منافسه لها في الأسواق العالمية أو التي قد تضر بالشركة ضررا بليغا إذا ما تم نشر تلك المعلومات .

## ٥ - المعاهدات و القوانين الخاصة بحماية حق الملكية الفكرية

و تعتبر حماية الملكية الفكرية هي من أكثر الحقوق التي يتم انتهاكها يوميا على شبكة الإنترنت او على كافة شبكات الاتصالات و المعلومات على مستوى العالم و عليه فوجود معاهدات دولية تمنع تلك الانتهاكات و إصدار كل دولة قوانين خاصة بها تعمل على حماية حقوق الملكية الفكرية كل ذلك يؤدي إلى

الحفاظ على تلك الحقوق من الانتهاك الذي يتم يوميا دون أي رادع يحمي أصحاب تلك الحقوق .

و سوف نعرض أولا للمعاهدات التي تم إبرامها في هذا المجال و سوف نعرض ثانيا لما تم إصداره من قوانين في هذا المجال و لكن عرضنا سيكون على مستوى الدول العربية في محاولة لمعرفة مدى تقدمنا الثقافي الذي أصبحت الكثير من الأمم المتقدمة تقيسه ما تقدمه الدولة من حماية في مجال حماية حقوق الملكية الفكرية .

أولا : - المعاهدات الدولية التي تم إبرامها في مجال حماية حقوق الملكية الفكرية

من أهم المعاهدات التي تم إبرامها في هذا المجال معاهدات ثلاث هم على التوالي : -

- ١ - معاهدة برن

- ٢ - معاهدة ترينيس

- ٣ - معاهدات الويبو

١ - معاهدة برن لحماية المصنفات الأدبية و الفنية

تعتبر معاهدة برن و التي تم التوقيع عليها في عام ١٩٧١ في سويسرا هي حجر الأساس في مجال الحماية الدولية لحق المؤلف و قد وقعت على هذه الاتفاقية ١٢٠ دولة من بينها جمهورية مصر العربية و تعد المادة التاسعة من

تلك الاتفاقية هي أساس في تلك الاتفاقية لأنها تنص على منح أصحاب حقوق المؤلف حق استثنائي في التصريح بعمل نسخ من هذه المصنفات بأي طريقة و بأي شكل كان .

وفضلا عن ذلك تمنح اتفاقية برن صاحب حق المؤلف الحق في أن يرخص أو يمنع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه وكذلك تلزم الاتفاقية بتوقيع جزاءات سواء أكان المؤلف المعتدى عليه وطنيا أم أجنبيا

## ٢ - معاهدة تريبس

### الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية

معاهدة تريبس هي الأخرى من المعاهدات التي تم إجازها في مجال حماية الملكية الفكرية من السطو عليها خصوصا مع انتشار عمليات السطو الإلكتروني على العمال الفنية دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية .

و تلك الاتفاقية تم التوقيع عليها من قبل الدول الأعضاء بها عام ١٩٩٤ و قد عالج موقعو الاتفاقية العامة للتعريفات و التجارة ( الجات ) حقوق الملكية الفكرية بتوقيع اتفاق الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية TRIPS فربطوا بذلك بين المعايير الدولية و المعايير المحلية و تتضمن تلك الاتفاقية العديد من الإجراءات الهامة و الفعالة لردع الاعتداءات على حقوق الملكية الفكرية كما أنها و من جهة أخرى تفرض على الدول اتخاذ العديد من التدابير الهامة لمعالجة الوضع و من تلك التدابير على سبيل المثال لا الحصر إعطاء الحق للسلطات في إصدار الأوامر بشن حملات مفاجئة لضبط أدلة

ارتكاب الجريمة و التي عادة ما تكون سهلة التخلص منها لو لم تكن هناك سرعة في محاولة ضبطها و كذلك التحفظ على أدوات ارتكاب الجرائم و ذلك فضلا عن فرض عقوبات جنائية رادعة .

و في حالة تراخي الدولة العضو عن اتخاذ مثل تلك الإجراءات أو أن تهما في تطبيق قوانينها الوطنية فإن المنظمة العالمية تعلن أن تلك الدولة لا تقوم بما عليها من واجبات في تطبيق الشروط و الإجراءات المنصوص عليها في المعاهدة و بالتالي تكون عرضة لان تتخذ ضدها العديد من الإجراءات العقابية من باقي الدول الأعضاء .

### ٣ - معاهدات الويبو

في البداية نوضح أن معاهدة الويبو تنقسم إلى ثلاث معاهدات هي : -

- معاهدة الويبو بشأن حق المؤلف
- معاهدة الويبو بشأن الأداء و التسجيل الصوتي
- معاهدة الويبو بشأن الحماية الدولية لحق المؤلف و الحقوق المجاورة

#### ١ - معاهدة الويبو بشأن حق المؤلف

تم التوقيع على تلك المعاهدة في ٢٠ ديسمبر عام ١٩٩٦ و تتكون من ثمانية عشر مادة و تبدأ بالديباجة ثم تتناول علاقة تلك المعاهدة بمعاهدة برن ثم تتعرض لنطاق تطبيق حماية حق المؤلف كحق التوزيع و التأجير و نقل المصنف إلى الجمهور و الالتزامات المتعلقة بالتدابير التكنولوجية و الالتزامات المتعلقة بالمعلومات الضرورية المتعلقة بالحقوق و مدة حماية المصنفات و الاستثناءات و التقييدات على تلك الحقوق و كذلك الحقوق و الالتزامات

المرتتبة على المعاهدة و دخول المعاهدة حيز التنفيذ الفعلي و أخيرا تعرضت المعاهدة للحفاظ عليها و نقضها سواء من قبل أحد أطرافها الموقعين عليها أو من إحدى الدول الغير موقعة عليها و لغاتها .

و تنص الجملة الأولى من المادة الأولى من المعاهدة الأولى على أن هذه المعاهدة اتفاق خاص بمعنى المادة ٢٠ من اتفاقية برن لحماية المصنفات الأدبية والفنية بالنسبة إلى الأطراف المتعاقدة من بلدان الاتحاد المنشأ بموجب تلك الاتفاقية .

وتنص المادة ٢٠ من اتفاقية برن على أن تحتفظ حكومات دول الاتحاد بالحق في عقد اتفاقات خاصة فيما بينها ما دامت هذه الاتفاقات تخول حقوقا تفوق تلك التي تمنحها هذه الاتفاقية أو تتضمن نصوصا لا تتعارض مع هذه الاتفاقية .

وكانت للنص السالف الذكر من للمادة الأولى من المعاهدة الأولى بالتالي أهمية خاصة في تفسير المعاهدة إذ أنه يبين أن تفسير المعاهدة الذي قد يؤدي إلى الحد من الحماية التي تمنحها اتفاقية برن يعتبر مرفوضا .

وتعطي المادة الرابعة من المعاهدة الأولى ضمانا إضافيا للالتزام باتفاقية برن بأكبر قدر ممكن إذ أنها تضم جميع الأحكام الجوهرية لاتفاقية برن بالإحالة إليها وتنص على أن ( على الأطراف المتعاقدة أن تراعي المواد من ١ إلى ٢١ والملحق من اتفاقية برن )

وتوضح المادة الثالثة أن اتفاقية برن تشير في ذلك السياق إلى وثيقة باريس لاتفاقية برن لسنة ١٩٧١

وينبغي قراءة تلك النصوص على ضوء أحكام المادة ١٧ من المعاهدة التي



سنناقشها لاحقاً وبناء على تلك المادة لا تكون المعاهدة متاحة للبلدان الأطراف في وثيقة باريس لسنة ١٩٧١ والبلدان الأطراف في أية وثيقة من وثائق اتفاقية برن فحسب بل بالنسبة أيضاً إلى كل دولة عضو في الويبو سواء كانت طرفاً في الاتفاقية أو لم تكن طرفاً فيها ويجوز لبعض المنظمات الدولية الحكومية أيضاً أن تصبح أطرافاً في المعاهدة .

وتحتوي المادة الثانية من المعاهدة الأولى بند ضمان مشابهها للبند الوارد في المادة ٢-٢ من اتفاق تريبس وتنص على أنه ليس في هذه المعاهدة ما يحد من الالتزامات المترتبة حالياً على الأطراف المتعاقدة بعضها تجاه البعض الآخر بناء على اتفاقية برن لحماية المصنفات الأدبية والفنية غير أن نطاق ذلك البند يختلف عن نطاق البند الوارد في اتفاق تريبس وينطوي الأخير على أهمية من وجهة نظر مادة واحدة على الأقل من اتفاقية برن تضم أحكاماً جوهرية أي المادة السادسة المتعلقة بالحقوق المعنوية إذ لا ينص اتفاق تريبس على أية حقوق أو التزامات فيما يتعلق بتلك المادة

## ٢ - معاهدة الويبو بشأن الأداء و التسجيل الصوتي

تم التوقيع على تلك المعاهدة في ٢٠ ديسمبر ١٩٩٦ و تقع تلك المعاهدة في أربع فصول يتناول الفصل الأول منها الأحكام العامة علاقة تلك المعاهدة بالمعاهدات و الاتفاقات الدولية الأخرى و التعريف و المستفيدون من الحماية بناء على تلك المعاهدة و كذلك المعاملة الوطنية .

أما الفصل الثاني فيتناول حقوق فناني الأداء معنويًا و ماليًا و حقوق الاستنساخ و التوزيع و التأجير و حق إتاحة الأداء المثبت .

أما الفصل الثالث فيتناول حقوق المنتجين كحق الاستنساخ و التأجير و التوزيع

و حق إتاحة التسجيلات الصوتية .

و يتناول الفصل الرابع الأحكام المشتركة فيتناول الحق في مكافأة مقابل الإذاعة أو النقل إلى الجمهور و التقييدات و الإستثناءات على هذا الحق و مدة الحماية و الالتزامات المتعلقة بالتدابير التكنولوجية و الالتزامات المتعلقة بالمعلومات الضرورية لإدارة الحقوق و أخيراً تم التعرض للإجراءات الشكلية .

### ٣ - معاهدة الويبو بشأن الحماية الدولية لحق المؤلف و الحقوق المجاورة

و تبدأ تلك الاتفاقية بمقدمة ثم تتناول الطابع القانوني للمعاهدتين الجديتين و علاقتهما بالمعاهدات الدولية الأخرى ثم تتناول الاتفاقية جدول الأعمال الرقمي و المعاهدات الجديدة ثم تتعرض الاتفاقية إلى أحكام أخرى عامة عن المعاهدتين الجديتين و أخيراً أعمال المتابعة بعد المؤتمر الدبلوماسي .

### ثانياً : - القوانين التي أصدرتها الدول العربية في مجال حماية حقوق الملكية الفكرية

أما بالنسبة لقوانين حماية الملكية الفكرية التي تم إصدارها فسوف نعرض لتلك القوانين التي صدرت على مستوى عالمننا العربي

### ١ - قانون حماية الملكية الفكرية الصادر بدولة الإمارات العربية المتحدة

وضعت دولة الإمارات العربية المتحدة في العام ١٩٩٢ قانوناً لحماية الملكية الفكرية بموجب القانون الاتحادي رقم (٤٠). وتشمل المواد التي تضمنها قانون

حقوق الملكية الفكرية برامج الكمبيوتر بالتحديد. وبالتالي يصبح نسخ المواد المحمية بموجب قانون حماية الملكية الفكرية من غير إذن أو توزيع نسخها عملاً غير قانوني . فلا يجوز صنع أية نسخ من غير إذن صريح من صاحب حق الملكية الفكرية

يمنع قانون دولة الإمارات العربية المتحدة نسخ برامج الكمبيوتر بدون إذن وكل من يقبض عليه متلبساً بقرصنة البرامج سيخضع هو وشركته للمحاكمة بموجب القانون المدني أو الجنائي وتشمل العقوبات حسب القانون غرامة مالية قدرها ٥٠٠٠٠ درهماً أو أكثر بالإضافة إلى مصادرة المنتجات والحبس لمدة تصل إلى ثلاث سنوات

مسؤوليات المستخدم : - إن أولى مسؤولياتك كمستخدم لبرامج الكمبيوتر هي أن تشتري البرامج الأصلية وإذا اشتريت البرامج لاستخدامها في أعمالك التجارية ينبغي أن يكون لكل جهاز كمبيوتر في شركتك مجموعته الخاصة من البرامج الأصلية

ولهذا ينبغي عليك أن تتأكد عند شراء برامج كمبيوتر من أن المنتجات التي تشتريها قانونية ذلك أن العديد من المنتجات المزورة تكون أحياناً مصممة بشكل تبدو فيه مشابهة لمنتجات الصانع الأصلي إلا أنها تكون متدنية الجودة وبالتالي فإن مشتري ومستخدمي البرامج المزورة أو المنسوخة يواجهون مجازفات لا مبرر لها تتمثل في : -

- ٢ - عدم وجود المستندات الضرورية التي تمكنك من استخدام البرنامج بشكل صحيح

- ٣ - عدم حصولك على الدعم التقني للمنتجات المتوفرة للمستخدمين المسجلين

- ٤ - عدم حصولك على البرامج المطورة التي يحصل عليها المستخدمون المسجلون

- ٥ - وبالإضافة إلى ذلك فإن شراء البرامج الأصلية يعنى أن جزءاً كبيراً من هذا الثمن سوف يخصص إلى برامج التطوير إلى تعنى بتقديم الجديد من البرامج الأسهل و الأكثر تطوراً بما يؤدي إلى تطور المنتجات و تحديثها و يؤدي إلى اللحاق بركب الدول المتقدمة تكنولوجياً هذا في حال شراء برامج أصلية أما عند شراء برامج غير أصلية فلا يكون هناك أي مخصصات لبرامج التطوير و تذهب تلك النقود إلى القراصنة الذين نسخوا تلك البرامج دون أن يبذلوا أي جهد في إنتاجها و دون أن يكون للشركات التي طورت و بحثت و أنتجت تلك البرامج أي نصيب من هذا الثمن مما يحرمها من الحصول عليه و بالتالي نقل الأموال التي يمكن إنفاقها على البحث و التطوير

و لقد اتخذت دولة الإمارات العربية المتحدة تدابير فعالة جداً لحماية حقوق الملكية الفكرية فقد نصت على عقوبات عديدة رادعة و قامت بحملات مدهامة عديدة من خلالها تم القبض على كم كبير جداً من البرامج الغير أصلية وإن حملات المدهامة هذه ضد قراصنة برامج الكمبيوتر مستمرة لتشجيع شراء

البرامج الأصلية.

## ٢ - قانون حماية الملكية الفكرية الصادر بالمملكة العربية السعودية

يوفر نظام حماية حقوق المؤلف لمصنفات الحاسب الآلي الحماية لمدة خمسون عاما من تاريخ وفاة المؤلف أو من تاريخ النشر إذا كان المؤلف شخصا مغنويا ويحظر القانون أي تقليد أو بيع أو إيجار أو توزيع أو استيراد أو تصدير أي مصنف دون إذن من مالك الحق .

الحقوق التي يتمتع بها المؤلف : -

بموجب هذا القانون يتمتع المؤلف بالحقوق الآتية : -

- ١ - استغلال مصنفه ماليا بأي طريقة من طرق الاستغلال المشروعة
- ٢ - نسبة مصنفه إلى نفسه ودفع أي اعتداء على حقه وله كذلك الاعتراض على كل تحريف أو تشويه أو تعديل أو تغيير لمصنفة أو كل مساس آخر بذات المصنف يكون ضارا بشرفه أو بسمعته
- ٣ - نشر مصنفة أو تسجيله أو عرضه أو نقله أو ترجمته و تقرير ما يتعلق بذلك من شروط وقيود
- ٤ - إدخال ما يراه من تعديل أو إجراء أو حذف على مصنفة
- ٥ - سحب مصنفة من التداول

العقوبات التي قررها القانون

- ١ - يعاقب المعتدى على حق المؤلف بغرامة عشرة آلاف ريال أو بإغلاق المؤسسة أو المطبعة التي اشتركت في الاعتداء أو بهما معا



- ٢ - بالإضافة إلى تعويض صاحب الحق عما لحقه من أضرار
- ٣ - في حالة العود يعاقب المعتدي بمضاعفة العقوبة السابق ذكره

### ٣ - قانون حماية الملكية الفكرية الصادر بدولة الكويت

أصدرت دولة الكويت القانون رقم ٩٩/٦٤ بشأن حماية حقوق الملكية الفكرية الذي يحمي برامج الكمبيوتر تحديداً وبموجب هذا القانون يعتبر نسخ المواد المتمتعة بحقوق الملكية الفكرية أو توزيع أو تأجير أو استيراد تلك النسخ بدون إذن من صاحبها عملاً غير قانوني فلا يجوز النسخ من غير إذن صريح من صاحب حق الملكية الفكرية إلا نسخة واحدة فقط لغرض المساندة.

العقوبات المقررة بموجب هذا القانون : - يمنع القانون الكويتي رقم ٩٩/٦٤ نسخ البرامج من غير إذن صاحب الحق وكل من يقبض عليه متلبساً بقرصنة البرامج سيخضع هو وشركته للمحاكمة وتشمل العقوبات حسب القانون غرامة مالية تصل إلى ٥٠٠ دينار كويتي أو الحبس لمدة قد تصل إلى سنة واحدة أو العقوبتين معاً وكذلك مصادرة المنتجات والتجهيزات المستخدمة في نسخ البرامج المزورة و إتلافها ونشر الحكم الصادر في المخالفة في وسائل الإعلام وعلى حساب المخالف وفي حال تكرار المخالفة خلال خمس سنوات من تاريخ الحكم السابق سوف تزداد العقوبة عن الحد الأقصى المقرر بما في ذلك إغلاق المنشأة لمدة قد تصل إلى ستة أشهر .

مسؤوليات المستخدم المنصوص عليها في القانون : - إن أولى مسؤولياتك كمستخدم لبرامج الكمبيوتر هي أن تشتري البرامج الأصلية وإذا اشتريت البرامج لاستخدامها في أعمالك التجارية ينبغي أن يكون لكل جهاز كمبيوتر في

شركتك مجموعته الخاصة من البرامج والوثائق المرفقة بها .

ولهذا ينبغي عليك أن تتأكد عند شراء برامج كمبيوتر من أن المنتجات التي تشتريها قانونية ذلك أن العديد من المنتجات المزورة تكون أحياناً مصممة بشكل تبدو فيه مشابهة لمنتجات الصانع الأصلي، إلا أنها تكون متدنية الجودة وبالتالي فإن مشتري ومستخدمي البرامج المزورة أو المنسوخة يواجهون مجازفات لا مبرر لها :

- ١ - الفيروسات أو الأقراص التالفة أو البرامج ذات العيوب الأخرى
- ٢ - عدم وجود المستندات الضرورية التي تمكنك من استخدام البرنامج بشكل صحيح
- ٣ - عدم حصولك على الدعم التقني للمنتجات المتوفرة للمستخدمين المسجلين
- ٤ - عدم حصولك على البرامج المطورة التي يحصل عليها المستخدمون المسجلون
- وبالإضافة إلى ذلك فإن شراء البرامج الأصلية يعنى أن جزءاً كبيراً من هذا الثمن سوف يخصص إلى برامج التطوير إلى تعنى بتقديم الجديد من البرامج الأسهل و الأكثر تطوراً بما يؤدي إلى تطور المنتجات و تحديثها و يؤدي إلى اللحاق بركب الدول المتقدمة تكنولوجياً هذا في حال شراء برامج أصلية أما عند شراء برامج غير أصلية فلا يكون هناك أي مخصصات لبرامج التطوير و تذهب تلك النقود إلى القراصنة

- الذين نسخوا تلك البرامج دون أن يبذلوا أي جهد في إنتاجها و دون أن يكون للشركات التي طورت و بحثت و أنتجت تلك البرامج أي نصيب من هذا الثمن مما يحرمها من الحصول عليه و بالتالي تقل الأموال التي يمكن إنفاقها على البحث و التطوير

لقد التزمت الحكومة الكويتية بحماية حقوق الملكية الفكرية و تقوم بحملات مداومة مفاجئة على القرصنة و فرض عقوبات رادعة على المخالفين تهدف إلى تشجيع إنتاج و شراء البرامج الأصلية .



## الفصل الرابع





## تجربة جمهورية مصر العربية في مكافحة جرائم الحاسبات و شبكات المعلومات

للحديث عن تجربة جمهورية مصر العربية في مجال مكافحة جرائم الإنترنت أو ما يطلق عليه الجرائم المعلوماتية لابد أن يكون بداية الحديث عن تلك القوانين التي لابد و أن تكون موجودة كأساس يتم بموجبه تحديد ماهية الأفعال التي تعتبر جرائم ففي كل الدول الحديثة المتقدمة تكنولوجيا و علميا و قانونيا يوجد قانون للعقوبات يحدد الجرائم التقليدية و أركانها كل انه يوجد أيضا قانون الإجراءات الجنائية و هو القانون الذي يقرر أساليب و وسائل الإبلاغ عن الجريمة التقليدية و الطرق المتبعة في التحري عن صحتها و مرتكبيها و جمع الاستدلالات عنها و ضبطها و التحقيق فيها ثم أخيرا إحالة المتهم بارتكابها إلى المحاكمة حيث تتم أدانته و يلقي العقاب المنصوص عليه في القانون جزاء ما ارتكبت يده أو يقضى ببراءته فيطلق سراحه .

كل ذلك يستلزم وجود الدليل المقبول قضائيا لإدانة ذلك المتهم و من القواعد الثابتة في قانون العقوبات في أي دولة

- انه لا جريمة إلا بنص

- لا عقوبة إلا بقانون

- أن الشك يفسر لصالح المتهم

و عليه فبعض الجرائم قد تتم بالأسلوب التقليدي العادي غير الإلكتروني فتقه تحت طائلة نصوص القانون السارية في الدولة و يلقي المتهم عقابه على ما ارتكبت يده .

أما جرائم الاعتداء على نظم و شبكات المعلومات و شبكات الاتصال و التي تقع بالشكل الإلكتروني غير التقليدي لا تتوافر لها حتى الآن نصوص قانونية سواء

ففي قانون العقوبات أو في قانون الإجراءات الجنائية لتجريمها و لتقرر العقوبة المقررة على كل جريمة تتم بهذا الشكل غير التقليدي .

هذا من جهة و من جهة أخرى فإن تلك الجرائم الإلكترونية تشمل في معظم الأحوال أفعالا ضارة تقع على نظم المعلومات و شبكات الاتصال و هو ما يؤثر بالسلب على التجارة الإلكترونية أو أي أعمال إلكترونية أخرى نظرا لان تلك الجرائم تكون أداة الجريمة فيها نظم الحاسبات و البرمجيات و من ثم فانه لكي تتوفر إمكانية تجريم تلك الأفعال و وضع العقاب على من يرتكبها لابد من توافر نصوص قانونية في قانون العقوبات و قانون الإجراءات الجنائية تجرم أفعال الاعتداء على نظم و شبكات المعلومات و الحاسبات و الاتصالات أي جرائم المجال الإلكتروني أو ما يطلق عليه جرائم الإنترنت أو أي أفعال اعتداء على الأشخاص و الأموال و التي تقع باستخدام وسائط إلكترونية بالإضافة إلى نصوص قانونية أخرى تبين ماهية الوسائل التي يتم استخدامها عند جمع الاستدلالات عن تلك الجرائم و ضبطها و الكيفية البحث عن الأدلة الخاصة بها و الحفاظ عليها و التحقيق في تلك الجرائم تمهيدا للقبض على مرتكبها لينال ما ارتكبت يداه من أفعال ضارة .

و يلزم قبل توافر تلك النصوص القانونية وجود الشرطة الفنية المدربة فنيا و تكنولوجيا على التعامل مع ذلك النوع من الجرائم التكنولوجية الحديثة فيلزم أن تكون أجهزة الشرطة مدربة فنيا بالقدر الكافي الذي يجعلها قادرة على ضبط تلك الجرائم و التعامل مع مرتكبيها و إيجاد الدليل الخاص بها و الحفاظ عليه و ليست أجهزة الشرطة فقط هي التي يجب أن تكون مؤهلة لذلك بل يجب أن يكون رجال النيابة العامة و رجال القضاء و السادة المحامين يجب أن يكونوا جميعا مؤهلين للتعامل مع ذلك النوع من الجرائم الإلكترونية الحديثة هذا من جهة و من جهة أخرى يلزم توافر الأجهزة الفنية لهم أيضا ليستطيعوا القيام بما

هو منوط بهم من واجبات إمكانية التعامل معها فالتدريب الفني فقط لا يأتي بالنتائج المرجوة بل لابد من وجود الأجهزة الفنية التي تعينهم على القيام بمهامهم .

هذا ولما كانت الجرائم الإلكترونية التي تقع علي نظم وشبكات الحاسبات والاتصالات في أحيان كثيرة جرائم عابرة للحدود **CRIMES TRANS BORDER** أي أن مرتكب الجريمة قد يستخدم حاسباً أو جهازاً أو شبكة اتصال في دولة وتقع الجريمة علي حاسب أو نظام أو شبكة اتصال في دولة أخرى فإن الأمر يستلزم وجود اتفاقية دولية تنظم هذه المسائل بين الدول حتى تعدل قوانين العقوبات وقوانين الإجراءات الجنائية في كل منها لتجريم تلك الأفعال - فلا يكون هناك أفعال معاقب عليها في دولة ما و لا يكون معاقب عليها في دولة أخرى و بالتالي تكون الفرصة سانحة أمام مرتكبي تلك الأفعال أن يفلتوا بفطنتهم باللجوء إلى الدول التي لا تجرم تلك الأفعال - و ذلك كي يتحقق التعاون الدولي بين الدول في تلك الجرائم فلا يفلت الجاني بفطنته علماً أن ذلك التنظيم موجود جزئياً من خلال ما يعرف بمعاهدة بودابست لمكافحة جرائم نظم وشبكات الاتصالات **THE BUDAPEST CONVENTION ON CYBER CRIMES** والتي لم تنضم مصر إليها حتى الآن.

و عليه ففي مجال عرضنا لتجربة جمهورية مصر العربية في مجال مكافحة جرائم الإنترنت سوف نعرض لعدة نقاط هي :

- ١ - إصدار قانون حماية الملكية الفكرية
- ٢ - تحديث القوانين السائدة إلى قوانين جديدة تجرم جرائم الإنترنت
- ٣ - الانضمام إلى المعاهدات و الاتفاقات الدولية التي تعمل على تجريم جرائم الإنترنت
- ٤ - استحداث قوانين جديدة تقن الاستخدامات الإلكترونية مثل قانون

- التجارة الإلكترونية و قانون التوقيع الإلكتروني
- ٥ - إنشاء إدارات جديدة بوزارة الداخلية تكون مسنولة عن تلك الجرائم
- ٦ - تحقيق الأمن المعلوماتي للكيانات الاقتصادية

## ١ - إصدار قانون حماية الملكية الفكرية

كانت جمهورية مصر العربية من أولى الدول العربية التي انضمت إلى كافة المعاهدات و الاتفاقات الدولية التي كانت تعمل في مجال حماية حقوق الملكية الفكرية من القرصنة و تأسيسا على هذا الاهتمام فقط انضمت مصر إلى معاهدة برن و تريبس و معاهدات الويبو و كان من نتيجة هذا الاهتمام أن أصدرت مصر قانون حماية الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٣ و الذي يوفر الحماية لمصنفات الحاسب الآلي لمدة خمسون عاما من تاريخ وفاة المؤلف أو من تاريخ النشر .

أما عن الحقوق التي يتمتع بها المؤلف طبقا لهذا القانون فقد نص القانون على تمتع المؤلف وحده بالحقوق في الترخيص أو عدم الترخيص لأي جهة باستغلال مصنفه سواء بالنسخ أو البيع أو التأجير أو الإعارة أو إتاحتها عبر أجهزة الحاسب الآلي و شبكة الإنترنت و غيرها من شبكات المعلومات و وسائل الاستغلال .

و يحظر القانون الآتي :

- أي نسخ كلي أو جزئي للبرامج أو الاقتباس منها إلا بعد الحصول ترخيص كتابي مسبق من المؤلف أو من الممثل القانوني له
- إزالة أو تعطيل أو التغيب لأي حماية تقنية يستخدمها المؤلف كالتشفير



- أو غيره
- تقليد أو بيع أو عرض للتداول أو للإيجار في مصر مصنفًا منشورًا في الخارج أو تصديره .
- النشر عبر أجهزة الحاسب الآلي أو شبكات الإنترنت أو شبكات المعلومات أو شبكات الاتصالات أو غيرها من شبكات و الوسائل دون إذن كتابي مسبق من المؤلف
- الاعتداء على أي حق أدبي أو مالي من حقوق المؤلف
- العقوبات التي تقررت بموجب قانون حماية الملكية الفكرية : -
- الجزاءات الجنائية : -
- يعاقب المعتدى بالحبس من شهر حتى ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف جنيه لكل برنامج أو بإحدى هاتين العقوبتين
- بإغلاق المنشأة التي استغلها المقلدون أو شركاؤهم كما يجوز للمحكمة أن تقضي مدة لا تزيد على ستة أشهر
- وفي حال معاودة المخالفة يصبح الحبس وجوبيا بحد أدنى ثلاث شهور مع غرامة مالية قد تصل إلى ٥٠ ألف جنيه ويصبح غلق المنشأة وجوبيا
- وتتم في كل الأحوال مصادرة النسخ المقلدة والأدوات المستخدمة في الاعتداء
- ينشر ملخص الحكم الصادر بالإدانة في جريدة يومية واحدة أو أكثر على نفقة المحكوم عليه
- الجزاءات المدنية : -
- يستحق المؤلف أو من يخلفه في حال الاعتداء على حق أو أكثر من حقوقه و الحصول على تعويضات مدنية عما لحقه من أضرار أدبية

- ومالية قد تصل إلى ملايين الجنيهات .
- يلزم القانون كل المحال التي تطرح للتداول بالبيع أو بالإيجار أو بالإعارة أو بالترخيص بالاستخدام مصنقات الحاسب الآلي أو قواعد البيانات بالحصول علي ترخيص بذلك من وزارة الاتصالات والمعلومات ويعاقب علي مخالفة هذه المادة بغرامة لا تقل عن خمسة آلاف ولا تزيد عن عشرين ألف جنيه مصري .
- يلزم القانون ناشرو وطابعو ومنتجو مصنقات الحاسب الآلي أو قواعد البيانات بإيداع نسخة من المصنف أو أكثر بما لا يجاوز العشرة ويعاقب علي مخالفة هذه المادة بغرامة لا تقل عن ألف جنيه ولا تزيد عن ثلاثة عن كل مصنف

## ٢ - تحديث القوانين السائدة إلى قوانين جديدة تجرم جرائم الإنترنت

### MODERNISATION THE REIGNING LAWS TO A NEW LAWS CRIMINALISING THE INTERNET CRIMES

حتى الآن لم يتم استحداث أي قوانين جديدة في جمهورية مصر العربية تجارى التطور الحادث في نوعية الجرائم و طرق ارتكابها - فحتى الآن يتم إدراج تلك الجرائم الإلكترونية التي ترتكب عبر شبكة الإنترنت تحت نصوص القوانين القديمة و يتم تطبيق العقوبات القديمة عليها رغم أن تلك الجرائم تحتاج إلى غلظة العقوبة حتى تكون المحاولة جادة في الحد من ارتكاب تلك الجرائم - و كان يجب أن تكون تلك القوانين قد تم سنها منذ أن انتشرت خدمة الإنترنت في

مصر على نطاق واسع لان انتشارها على نطاق واسع سيؤدي بالطبع إلى زيادة الاحتمال باستخدامها استخدما سينا في ارتكاب الجرائم الجديدة على المجتمع و بالتالي كان يجب أن تكون تلك القوانين جاهزة للتطبيق لا أن يتم التفكير في سنها بعد أن زاد ارتكاب تلك الجرائم بكافة أنواعها .

إلا انه في نفس الوقت لابد من الإشارة إلى أن ارتكاب تلك الجرائم لازل في مراحله الأولى رغم الانتشار السريع للإنترنت في مصر نظرا لطبيعة المصريين و ما يحكمهم من عادات و تقاليد تحد كثيرا من أي نزعات إجرامية قد تكون موجودة في أي فئة من فئات البشر فالطبيعة السمحة و تقربهم من الدين و التزامهم بأوامره و نواهيته تعمل على الحد من نسبة ارتكاب الجرائم عنها في أي بلد من بلاد العالم مهما يتاح لهم من وسائل ارتكابها .

و عملية تحديث القوانين لا تتم في جمهورية مصر العربية بالسرعة المطلوبة لتجارة التطور الحادث في التكنولوجيا و وسائل الاتصال و عمليات التجارة الإلكترونية و ما إلى ذلك من تطور حاصل في كافة المعاملات التي تتم باستخدام أحدث ما وصل إليه العالم من التكنولوجيا و سوف نعرض فيما يلي بعض من أهم القوانين التي لا يجب التأخر في عمليات التحديث الخاصة بها حتى لا نبتعد عن عمليات التطور التي تحدث يوميا و لكي لا تزداد الهوة التكنولوجية التي تعمل على زيادة الفارق فيما بين الدول المتقدمة و الدول النامية .

و من أهم القوانين التي تحتاج إلى تحديث :

١ - تلك القوانين التي تتعلق بمأموريات الشهر العقاري و التوثيق و اللوائح الخاصة بها و أهمية تحديث تلك القوانين و اللوائح لكي تتواءم مع المعاملات الجديدة - المعاملات الإلكترونية - و من نواحي التحديث التي يمكن طرحها انه يمكن اعتماد مصلحة الشهر العقاري و التوثيق لتصبح هي الجهة المؤتمنة علي

حفظ الوثائق الإلكترونية واعتمادها - الطرف الثالث المحايد المودع لديه الوثيقة - أو يمكن إيجاد جهات حكومية أخرى تتسم بالنزاهة والحيدة كهيئة البريد للقيام بتلك المهمة .

٢ - تحديث القوانين المنظمة لهيئة سوق المال و كذلك القوانين المنظمة للبورصات و اللوائح الخاصة بها و ذلك لأمر هام حيث انه من الضروري تحديث التعاملات التي تتم على الأسهم و السندات ليكون في الإمكان التعامل على الأسهم و السندات المصرية بالأساليب الإلكترونية الحديثة و بالتالي يمكن جذب رؤوس الأموال الأجنبية للاستثمار في مصر حيث انه بدون تحديث تلك القوانين و تقنين الأساليب الحديثة الإلكترونية ستتعاظم الفوارق التي تفرق بيننا و بين الدول المتقدمة تكنولوجيا .

٣ - نوع آخر من القوانين لابد من التعامل معه بمزيد من الأهمية لأنه يؤثر كثيرا مع رؤوس الأموال الأجنبية التي لابد من جذب الكم الأكبر منها إلى مصر فالتشريعات و اللوائح الضريبية لابد من تحديثها ليكون في إمكانها العمل في عصر يتم التعامل التجاري فيه إلكترونيا دون أي يرى أي من أطرافه الطرف الآخر و عليه فلا بد من تحديث تلك التشريعات التي تحكم المجال الضريبي في مصر ليجاري التطور الجاري في المجال التجاري الدولي و إلا فلن تتمكن الدولة من تحصيل ما تستحقه من حقوقها الضريبية على ما يتم من معاملات تجارية تتم إلكترونيا دون أن تكون الدولة قادرة على متابعتها و بالتالي تقف القوانين عاجزة عن أن تحصل حقوق الدولة .

٤ - أما عن التشريعات الجمركية فالحال مع التشريعات الضريبية هو نفسه الحال مع التشريعات الجمركية إذ انه لابد من تحديث تلك التشريعات الجمركية أيضا و بالتوازي مع التحديث الذي يجب إتمامه مع التشريعات الضريبية بل و مع كافة التشريعات الأخرى التي يتم تحديثها فالتأخير في تحديث تلك التشريعات



يؤثر على التعاملات التجارية التي تتم بين مصر و العالم الخارجي الذي أصبح التعامل بينه و بين بعضه الآخر إلكترونيا صرفا دون أن يكون فيه أي دور لتلك التشريعات القديمة التي عفي عليها الزمن .

٥ - لما كان لا يمكن الفصل بين التعاملات الداخلية التجارية التي تتم داخل البلد الواحد و بين التعاملات التجارية التي تتم بين الدول كان من اللازم تحديث تلك القوانين الداخلية التي قد يرى البعض انه لا فائدة كبيرة من تحديثها و هو رأى خاطئ لان التعاملات التجارية الداخلية هي امتداد طبيعي للمعاملات التجارية الخارجية و عليه فتحديث القوانين التي تستخدم في التعاملات التجارية في داخل مصر هو أمر ذو أهمية قصوى و من تلك القوانين قانون المناقصات و المزايدات و التوريدات و أهمية ذلك التحديث ليكون هناك توافقا و تلاهما بين تلك القوانين و طبيعة التجارة الإلكترونية

٦ - أما التشريعات الخاصة بحماية المستهلك في مجال التجارة الإلكترونية فهي من أهم التشريعات التي يجب أن تكون لها الأولوية في التحديث لان تحديث القوانين في كافة المجالات هدفه الأول هو تقوية الاقتصاد الوطني و هدف تقوية الاقتصاد الوطني هو تحسين الحالة الاقتصادية للمستهلك لأنه الأساس في كل ذلك و بالتالي فإن القوانين التي تستهدف حماية المستهلك هي الأولى في أن تنال الأولوية في التحديث لا أن يتم إدارها و إهمالها و إغفال دورها في حماية المستهلك .

٧ - تعديل قانوني العقوبات والإجراءات الجنائية ليكون النص فيهما صريحا على تجريم جرائم الإنترنت و الحاسبات الآلية بدلا من إدراج تلك الجرائم تحت النصوص القانونية القديمة و تحت مسمى الجرائم التقليدية القديمة لعدم وجود نصوص قانونية جديدة تنص صراحة و بوضوح على تجريمها .

فيكون هناك نصوص تنص صراحة على تجريم التشهير عبر الإنترنت و



نصوص أخرى تجرم الاحتيال عبر الإنترنت و أيضا أفعال الاعتداء علي نظم وشبكات الحواسيب المعلوماتية والاتصالات أو استخدام تلك الوسائل والتكنولوجيا الحديثة في الاعتداء علي الأشخاص والأموال وكذلك الدولة و الأفراد و الهيئات أو الشركات و النصب والغش والاحتيال والقرصنة المعلوماتية و هكذا تكون هناك نصوص تنص صراحة علي تجريم أي جرائم يمكن أن ترتكب عبر الإنترنت إلا انه يجب أن تراعى أيضا أن تكون تلك النصوص قد صيغت علي أساس أن تستوعب أي تطوير قد يحدث في المستقبل - على الأقل القريب - في طرق و وسائل ارتكاب مثل تلك الجرائم .

كما انه من المستحسن علي النص صراحة علي الأساليب التي يجب أن تتبع عند جمع الاستدلالات و التفتيش و التحقيق و ضبط وحفظ الأدلة الجنائية في الجرائم المعلوماتية تحديداً للمسئولية الجنائية وحماية للتجارة الإلكترونية والمعاملات الإلكترونية

هذا من جهة و من جهة فلابد من من تنظيم الدورات التعليمية الكافية لرجال البحث القضائي و أعضاء النيابة العامة و أعضاء الهيئات القضائية و كذلك السادة المحامون لتدريبهم علي الوسائل و الأدوات الإلكترونية لفهما و استيعابها ليتمكنوا من القيام بما هو منوط بهم في أعمالهم علي الوجه الأكمل دون أي تقصير .

### ٣ - الانضمام إلى المعاهدات و الدولية التي تعمل علي مكافحة جرائم الإنترنت

كانت حكومة جمهورية مصر العربية علي قناعة تامة و منذ البداية علي أن الانضمام إلى المعاهدات و الاتفاقات الدولية هو من أهم الوسائل التي يجب

الأخذ بها و اتباعها في مجال مكافحة جرائم الإنترنت و عليه فلم تتوان مصر في الانضمام إلى كافة المعاهدات الدولية التي تم عقدها في هذا المجال و ذلك إيماناً منها بأن الانضمام إلى الأسرة الدولية هو من أهم الوسائل التي يجب اتباعها في مجال مكافحة جرائم الإنترنت .

و يجب أن نربط هنا بين التعاون الدولي في مكافحة جرائم المعلومات و ما تقوم به مصر من خطوات هامة في هذا المجال فالتعاون الدولي الهام يتمثل في أوضح و أهم صورته في المعاهدات و الاتفاقات الدولية التي يتم عقدها سواء في مجال مكافحة جرائم الإنترنت و أيضاً في مجال حماية الملكية الفكرية و قد انضمت مصر إلى الاتفاقات الدولية الخاصة بحماية حق الملكية الفكرية كما أنها أصدرت قانون حماية الملكية الفكرية الخاص بها و الصادر برقم ٨٢ لسنة ٢٠٠٣ و قد كانت المعاهدات الدولية كمعاهدة برن و معاهدة تريبس و معاهدات الويبو هما الأساس الذي تم بناء عليهم من هذا التشريع الذي تنضم به مصر إلى الأسرة الدولية في مجال حماية الملكية الفكرية .

و من جهة أخرى فقد قامت مصر أيضاً بمسايرة الأسرة الدولية فيما تبنته هيئة الأمم المتحدة من إصدار قوانين خاصة بالتجارة الإلكترونية و التوقيع الإلكتروني و قد تم ذلك أيضاً إيماناً من مصر بأن الانضمام إلى المجتمع الدولي فيه الخير و الفائدة إلى جمهورية مصر العربية .

و مثال ذلك أيضاً انضمام مصر إلى كافة الاتفاقات العربية التي أقرها مجلس وزراء الداخلية العرب و كذلك مجلس وزراء الداخلية و العدل العرب و هي اتفاقات عربية تهدف إلى التعاون فيما بين الدول العربية في مجال مكافحة الجريمة المنظمة و الاتجار في المخدرات و المؤثرات العقلية و مكافحة الإرهاب .

#### ٤ - استحداث قوانين جديدة تقنن الاستخدامات الإلكترونية مثل قانون التجارة الإلكترونية و قانون التوقيع الإلكتروني

تلعب التجارة الإلكترونية **ELECTRONIC COMMERCE** بصفة خاصة و التطور الهائل في تقنيات الاتصال و المعلومات بصفة عامة دورا اقل مما يوصف بأنه هائل جدا في تطور الاقتصاد العالي بصفة عامة و الاقتصاد الوطني بصفة خاصة فلا يمكن إنكار أن التجارة الإلكترونية عملت و بشكل كبير جدا على سرعة انتقال المعاملات و رؤوس الأموال و ألغت ما كان يعوقها قديما من الحواجز الجغرافية التي كانت تحد كثيرا من حركتها و كذلك قلة المعلومات التي كانت تعتبر في الماضي الحاجز الأكبر في عدم اجتياز اقتصاد الدول النامية في النفاذ إلى العالمية و الحصول على نصيبه الطبيعي من حجم التجارة الدولية .

إلا انه و من جهة أخرى فإن التفاوت التكنولوجي فيما بين الدول المتقدمة و الدول النامية قد يؤدي إلى عدم استفادة اقتصاد الدول النامية من ذلك التقدم التكنولوجي الهائل الذي يعيشه العالم حاليا و المسمى التجارة الإلكترونية و عليه فصحيح أن الحواجز التي كانت تعوق الدول النامية قد زالت إلا انه قد وجد مكانها حاجز آخر ألا وهو التقدم التكنولوجي الذي يعتبر اسهل ولو جزئيا في إمكانية تجاوزه و العمل على التفوق فيه مع أهمية ملاحظة أن عدم قدرة الدول النامية على تجاوز مثل هذا الحاجز فسوف تزيد الهوة فيما بينها و بين الدول المتقدمة و أن يفيد عندئذ أي مجهود قد يبذل للعمل على تقليله .

هذا و يعد الإنترنت هو القوة الدافعة في انتشار التجارة الإلكترونية **ELECTRONIC COMMERCE** و بعد ما وفرته شبكة الإنترنت من سرعة قصوى في تناقل البيانات و الأموال و الوثائق في اقل من ثواني

قليلة مهما كانت المسافة التي تفصل بين الأطراف فشبكة الإنترنت تعد هي الوسيلة الوحيدة في إبرام الصفقات في الكثير جدا من الصفقات في الوقت الحالي .

و رغم أن العديد من الدول النامية لم تستفيد حتى الآن من تلك التكنولوجيا المتطورة نظرا لعدم وجود البنية التحتية لخدمات الاتصالات الهاتفية إلا أن جمهورية مصر العربية ليست كذلك .

فجمهورية مصر العربية لديها بنية تحتية متكاملة جدا في مجال الاتصالات الهاتفية و هو ما جعلها تستفيد أقصى استفادة و جعل انتشار شبكة الإنترنت INTERNET يتضاعف سنويا بل انه قد يكون يتضاعف أكثر من مرة في العام الواحد .

و يمثل ذلك في زيادة الخدمات الهاتفية في مصر خلال السنتين الأخيرتين بنسبة كبيرة لتصل عدد الخطوط الثابتة إلى ٨,٦ ملايين خط تليفوني بزيادة شهرية قدرها ٨٠,٠٠٠ خط جديد كما زادت نسبة انتشار التليفون المحمول في مصر لتصل إلى ٥ % سنويا أي ٥,٣ ملايين مشترك وهذا يرجع إلى اهتمام الحكومة المصرية بتطوير البنية الأساسية للمعلومات والاتصالات الهاتفية فمذ عام (١٩٨٥) اتخذ قرار لإنشاء البنية الأساسية للمعلومات الوطنية لتصبح الأساس لتطوير جميع القطاعات والصناعات بمشاركة القطاع العام مع القطاع الخاص، وخلال الفترة من ٨٥ - ٩٥ تم إنشاء أكثر من ٦٠٠ مركز لدعم واتخاذ القرار في ٢٦ محافظة بهدف تطوير التجارة والحياة الاقتصادية والاجتماعية.

كما أن مصر تنظر إلى التجارة الإلكترونية ELECTRONIC COMMERCE كداعم أساسي للتجارة وخطط التقدم الاجتماعي والاقتصادي حيث تقدم التجارة الإلكترونية فرصا لزيادة حجم التجارة وتنشيط



الاستثمار وتسهيل الصفقات التجارية بالإضافة إلى أنها تتيح أسواقاً أكبر وأكثر تنوعاً وطرقاً تسويقية جديدة ويتوقع أن يصل حجم التجارة الإلكترونية إلى أكثر من تريليون دولار أميركي وهذه الزيادة في حجم التجارة تحمل في طياتها مزايا كامنّة للاقتصاد المصري إذا استطاع استخدامها جيداً وخاصة بالنسبة للمشروعات الصغيرة والمتوسطة والتي قبل استخدام التجارة الإلكترونية كانت تفتقر السبل لترويج منتجاتها بالخارج.

كما أنه من المعروف أن التجارة الإلكترونية لا تقتصر فقط على التجارة و إنما تمتد لتشمل قطاعاً كبيراً من الأعمال كالخدمات المالية كالتأمين و البنوك و التجارة و السياحة و الترفيه و الدعاية و التسويق و المعلومات و التعليم و التدريب و الإعلام كالكتب الإلكترونية .

و ستكون التجارة الإلكترونية موجودة في بيئة صحيحة و ليتم الاستفادة منها أقصى استفادة فقد قامت مصر باتخاذ عدد من الخطوات نوجزها فيما يلي : -

- و قد تم إصدار قانون يقن التجارة الإلكترونية في مصر
- و كذلك أصدرت قانون آخر لتقنين مسألة التوقيع الإلكتروني
- تطوير البنية الأساسية للمعلومات بإنشاء العديد من مراكز المعلومات على مستوى الجمهورية
- تنفيذ العديد من المشروعات التي تعتمد و بشكل أساسي على الصناعات ذات التكنولوجيا العالية لنقل تلك التكنولوجيا إلى داخل مصر

- زيادة الوعي من جميع الجهات المعنية بالاستفادة من تلك التكنولوجيا المتقدمة و العمل على فتح منافذ للصناعات المصرية عبر تلك البوابة الإلكترونية التي تختصر الكثير من الوقت و المسافات .



ورغم أن مصر قد خطت الكثير من الخطوات في مجال التجارة الإلكترونية و تنشيطها و الاستفادة منها إلا أن الأمن هو من اكبر المشاكل التي تعرقل مثل هذه الخطوات .

فالحفاظ على السرية والخصوصية هو من أهم المشكلات التي تواجه التجارة الإلكترونية ليس في مصر فقط بل في العالم اجمع .

فلا بد من التأكيد على السرية و الخصوصية فيما يتعلق بالبيانات و المعلومات التي يتم تداولها على شبكة الإنترنت في مجال التجارة الإلكترونية و لابد من النص قانونا على الحفاظ على تلك السرية إذا أردنا على الاستفادة .

ورغم أننا نطالب بالنص قانونا على الحفاظ على السرية إلا أن تلك السرية يمكن أن تنتهك عبر الشبكة دون إمكانية التحقق من الهوية .

فعدم القدرة على التأكد من هوية المستخدم والتحقق من المعاملات من أكبر المشاكل التي تواجه التجارة الإلكترونية ويعتبر النقص في تحديد الهوية من الأسباب الرئيسية لتسهيل الاحتيال والخداع ويمكن أن يؤدي إلى جرائم عديدة لا يمكن ارتكابها في الأسواق التقليدية بنفس الطريقة فالاحتيال عن طريق كروت الائتمان يمكن أن يظهر عندما يطلب التجار دليلا حقيقيا والذي لا يمكن أن يمتلكه إلا المالك الحقيقي .

كما أن النظام الورقي البنكي الحالي يعوق التجارة الإلكترونية ولا يوجد ما يعوق البنوك بشكل قانوني من استخدام الإنترنت ولكن بسبب المخاوف المتعلقة بالأمن فإنهم لا يشعرون بالراحة من تبادل الصفقات و البيانات عبر الإنترنت لذلك فإن البنوك لا تقبل الدفع عبر الإنترنت ولا تبادل الصفقات حتى لو لم يكونوا ممنوعين بشكل رسمي من ذلك ويرجع الرفض السائد لدى البنوك المصرية في تسهيل الائتمان عبر الإنترنت والتبادل التجاري لنقص ضمان السرية و الأمن بخصوص إجراء تلك العمليات كما أن أعمال البنوك المحدودة

عبر الإنترنت كانت مقصودة ولكن إضافة إلى ذلك فقد تم التبليغ عن بعض عمليات الاحتيال التي تمت و لم يتم تحديد هوية مرتكبيها .

## ٥ - إنشاء إدارات جديدة بوزارة الداخلية تكون مسئولة عن تلك الجرائم

أنشأت وزارة الداخلية في جمهورية مصر العربية إدارة جديدة تماما في تكوينها و نوعية عملها جديدة في تكوينها لأنها تتكون من ضباط على أعلى درجة من التخصص و الحرفية في تكنولوجيا الحاسبات و شبكة الإنترنت و جديدة في نوعية عملها على أساس أن عملها ليس ضبط المجرمين التقليديين الذين لا زالوا يرتكبون جرائمهم بالطرق التقليدية القديمة المحفوظة لدى كافة العاملين بوزارة الداخلية المصرية و إنما لملاحقة مجرمين على درجة تقنية عالية في مجال الحاسبات و شبكة الإنترنت و يرتكبون جرائمهم بطرق متطورة على المجتمع مستخدمين فيها تكنولوجيا الحاسبات و شبكة الإنترنت و يكون من الصعب أن لم يكن من المستحيل أن تتم ملاحقتهم إلا باستخدام وسائل أكثر تطورا و بواسطة ضباط على أعلى درجة من التدريب و التخصص على تلك التكنولوجيا .

و قد تم إنشاء تلك الإدارة الجديدة بعد أن زاد عدد مستخدمي شبكة الإنترنت خاصة بعد أن أصبح الدخول على الشبكة يتم بسهولة كبيرة جدا و لا يحتاج إلى أي تعقيدات كما كان في أول الأمر عندما كانت في بدا دخولها إلى مصر إذ أن الدخول على شبكة الإنترنت الآن لا يحتاج إلا إلى خط تليفون و جهاز كومبيوتر بالطبع .

و بالطبع و مع زيادة عدد مستخدمي الإنترنت زاد بالتالي من يقومون باستخدام تلك التكنولوجيا استخداما سيئا و يستغلونها في ارتكاب جرائمهم معتقدين انهم بعيدون جدا عن أيدي القانون و بعيدين عن أن ينالوا عقابهم على ما ارتكبت أيديهم فعدد الجرائم التي ترتكب باستخدام تلك الشبكة و عليه كان من الضروري إنشاء تلك الإدارة ليكون في الإمكان الحد من تلك الجرائم و محاولة منعها نهائيا أن أمكن

و قد تلاحظ أن معظم تلك الجرائم التي ترتكب على الشبكة أو باستخدام الحاسبات يكون تكييفها القانوني متوافق في معظم الأحيان مع التكييف القانوني التقليدي المنطبق على نفس الجرائم التي ترتكب بالطرق التقليدية مع وجود فراق واحد فقط هو أداة الجريمة أي استخدام الحاسبات أو شبكة الإنترنت INTERNET في ارتكاب الجريمة أي استخدام التقدم التقني MODERN TECHNIQUES في ارتكاب الجرائم بدلا من الطرق التقليدية التي كانت تلك الجرائم ترتكب بها دائما في الماضي و هو بالتالي ما يضعها تحت طائلة القانون LAW دون الحاجة إلى وجود نصوص قانونية جديدة تجرم تلك الجرائم CRIMES .

و وجد أن معظم ما تم ضبطه من جرائم هي في الغالب جرائم ابتزاز و تشهير و نصب و احتيال و سرقة و دعارة و إنما هي تتم بطرق تكنولوجية حديثة لم يكن في الإمكان كشفها و ملاحقة مرتكبيها أو ضبطهم إلا بوجود تلك الإدارة التي تم إنشائها حديثا .

و نحن نرى أن من أهم ما قامت به تلك الإدارة هو ملاحقة القائمين على المواقع الإباحية التي يتم بثها من داخل البلاد فتلك المواقع بما تبثه من سموم تعمل على إثارة الغرائز فتؤدي إلى ازدياد الجرائم الجنسية و إغلاق تلك المواقع و ملاحقة القائمين عليها يعمل على الحد من الجرائم الجنسية التي تقع

بمسبب زيارة تلك المواقع و ما تقوم به من إثارة الغرائز لدى الشباب بصفة خاصة و الرجال بصفة عامة

و نحن نرى أيضا أن وجود نصوص قانونية يتم تطبيقها على تلك الجرائم الحديثة **MODERN CRIMES** لا يقضى عن الحاجة إلى وضع نصوص قانونية جديدة و متطورة تغطى تلك الجرائم الجديدة و ما قد يستجد عليها من جرائم فالتطور التقني **MODERN TECHNIQUES** الذي نعيشه حاليا و الذكاء و درجة التقنية العالية التي يكون عليها هؤلاء المجرمين تنبأ بأنه و في المستقبل القريب سنواجه العديد من الجرائم شديدة التعقيد و التطور و التي لا تجد لها نصا قانونيا تقع تحت طائلته من تلك النصوص القانونية التقليدية القديمة التي نضع الجرائم التي ترتكب حاليا في نطاقها فنحن في حاجة إلى نصوص قانونية جديدة بحيث تجرم تلك الجرائم التكنولوجية الجديدة و ما قد يستجد عليها من جرائم و من تطور في أدوات ارتكاب مثل تلك الجرائم حتى لا يأتي الوقت الذي تقف فيه يد القانون عاجزة عن أن تقتص حق المجتمع من تلك الفئة المنحرفة التي تستغل التكنولوجيا الحديثة و التطور التقني **MODERN TECHNIQUES** في ارتكاب الجرائم بدلا من استغلالها في ما يفيد المجتمع و الاقتصاد الوطني .

على انه يمكن أن تتم الاستعانة عند وضع مثل هذا القانون الجديد بالقوانين التي وضعتها الدول المتقدمة في هذا المجال للعمل على توحيد القوانين التي تعالج تلك الجرائم في جميع الدول و ذلك في محاولة للحد من مثل تلك الجرائم ليس على المستوى المحلى فقط و إنما على المستوى العالمي أيضا .

وفى هذا المجال يمكن أن يكون للأمم المتحدة الدور الريادي في ذلك فليها أن تتصدى لمثل هذا الموضوع بأن تعمل على وضع قانون نموذجي موحد **UNIFIED MODEL LAW** بحيث يكون على الدول عند وضع قانونها



المحلى أن تقتبس منه ما هو مناسب لمجتمعها و تقاليدها و بالتالي يكون هناك الحد الأدنى على الأقل في التماثل و التناسق بين القوانين التي تعالج هذا الموضوع على المستوى العالمي وهو ما يعمل على الحد من ارتكاب مثل تلك الجرائم و أيضا لابد من وجود تناسق في القوانين لمواجهة الجرائم التكنولوجية الحديثة التي تكون في الأغلب الأعم من الحالات هي جرائم عابرة للحدود **CRIMES TRANS BOEDER** و لمواجهةها لابد من وجود مواجهة لها من كافة القوانين الموضوعية على المستوى المحلى و الدولي .

## ٦ - تحقيق الأمن المعلوماتي للكيانات الاقتصادية

تعد الكيانات الاقتصادية متمثلة في الشركات و البنوك و ما شابه ذلك من الركائز التي يرتكز عليها أي اقتصاد وطني و عليه فحماية الأمن الإلكتروني لتلك الكيانات هو من الأولويات التي يجب تحقيقها في الاعتبار على وجه السرعة و دون أي إبطاء قد يتسبب في اختراق تلك المنشآت و ما قد يتسبب فيه ذلك من خسائر مادية و معنوية هائلة لتلك المنشآت و مستوى سمعتها العالمية من الثقة و الأمان .

و عليه فقد تمت دراسة المحاولات التي يمكن بذلها لاختراق تلك الكيانات الاقتصادية و الحلول التي تم وضعها لمنع حدوثها

## ١ - محاولات الاختراق

١ - أن ضغط المعلومات على وسيط معلوماتي في حيز دقيق هو بالقطع أمر مفيد للمنشأة ولكنه قد يصبح عنصر خطر فالأسرار التجارية المالية والصناعية



يتم تخزينها في وسائط معلوماتية مضغوطة دقيقة الحكم يسهل سرقتها وإخراجها من المنشأة في حيز لا يزيد علي عتبة السجائر كما يمكن نقل المعلومات المالية والتجارية والصناعية المخزنة إلكترونياً في لحظات معدودة غير شبكات الحواسيب والاتصالات.

٢ - إن اللامركزية في حفظ واسترجاع المعلومات الحساسة إلكترونياً لها مخاطرها ففي بعض المنشآت يكون للعاملين حرية وقدرة الدخول إلي نظم المعلومات والاتصالات الخاصة بشبكة حواسيب المنشأة ويمكن لهم في حالة عدم وجود نظام أمن معلومات وأمن اتصالات أن يغتربوا مثل هذه المعلومات وأن يستخدموها بشكل غير أمين أو غير مشروع يضر بالمنشأة.

٣ - إن استخدام وسائل الاتصالات غير المشفرة لنقل رسائل البيانات الإلكترونية وغيرها من المعلومات يعرض المنشأة التجارية لمخاطر أنشطة إجرامية من منشآت منافسة .

٤ - إن سهولة نقل المعلومات باستخدام البرمجيات ووسائل الاتصالات الحديثة دون تأمين أدوات المعلومات والاتصالات يعرض أسرار المنشأة التجارية لمخاطر جسيمة.

٥ - أن تحرك وتنقل وسفر المسئولين عن المنشأة التجارية بأجهزة حاسبات نقالة غير مؤمنة تحتوي علي معلومات دقيقة وحساسة خاصة بالمنشآت وأنشطتها التجارية والمالية يعرض تلك البيانات والمعلومات لمخاطر في حالة سرقة تلك الأجهزة أو الدخول إليها من شخص غير مرخص له .

٦ - أن عدم تأمين نظم الاتصالات والحاسبات والمعلومات يعرض ممتلكات الشركة وبياناتها للتخريب والتدمير خاصة في حالة عدم وجود نظم حفظ بديلة .

٧ - إن استخدام المقاولين من خارج المنشأة SURCING OUT في

عمليات إنشاء أو حفظ أو إدارة نظم الحاسبات والمعلومات والاتصالات الخاصة بالمنشأة قد يعرض المنشأة لمخاطر جسيمة وقد يعرض أسرارها لمخاطر لا يعرف مداها سواء عن طريق الموظفين التابعين لذلك المقاول أو المقاول ذاته سواء كان موجوداً في الموقع - ركز المنشأة - أو يتعامل ويتصل بالنظام من خارج المنشأة و عليه لابد من التأكد من السمعة الممتازة لهؤلاء المقاولين قبل إسناد تلك العمليات لهم مع مراقبة تنفيذ الأعمال بواسطة استشاري متخصص محايد وحسن السمعة .

٨ - إن الإدارة التي ليست على قدر من الكفاءة لتدير نظم وشبكات المعلومات والاتصالات داخل المنشأة قد تعرض بيانات المنشأة وممتلكاتها لمخاطر جسيمة ومن ذلك الاختراق من قبل أشخاص أو جهات علي مستوى احتراف عال أو من موظفين من ذات المنشأة .

٩ - أن ضعف الوعي بأمن المعلومات وآمن الاتصالات في المنشأة قد يكون مصدر خطر ففي المنشأة الكبرى قد يوجد مسئولين أكفاء عن أمن المعلومات و أمن الاتصالات ولكن في الشركات متوسطة الحجم أو المنشأة الفردية قلما يوجد متخصص في أمن المعلومات و أمن الاتصالات.

إضافة إلي الاختراق المادي الملموس لنظم ومنشآت الحاسبات والاتصالات المتمثل مثلاً في سرقة وسائط إلكترونية مشحونة بالبيانات أو تكسير المعدات أو إتلافها الخ فإن من الوسائل الفنية للاعتداء علي نظم المعلومات والاتصالات ما يلي :-

١ - اختراق شبكات الاتصالات بوسائل مادية بالدخول إلي الخط التليفوني الواصل بالمنشأة عبر وصلة سلكية مادية وذلك للحصول علي معلومات صوتية أو بيانات منقولة .

- ٢ - التصنت علي المكالمات التليفونية باستخدام وسائل فنية مثل DIALER NUMBER RECORDER ( DNR )
- ٣ - استخدام وسائل مثل جهاز مسح الموجات SCANNER للتصنت علي الاتصالات الخاصة بالمحمول وخلافه.
- ٤ - وضع أجهزة تنصت في أجهزة الحاسبات أو الاتصالات الخاصة بالمنشأة أو في غرف اجتماعاتها.
- ٥ - عدم الكشف علي البرمجيات التي يتم إعدادها للمنشأة من قبل مهندسي برمجيات للتأكد من وجود أو عدم وجود أوامر نائمة أو مدفونة لإساءة استخدام البرمجيات في الحال والاستقبال عند تشغيل تلك البرمجيات.
- ٦ - وجود ثقب HOLE أو ثقب في نظم الحاسبات أو البرمجيات قد يؤدي إلي إمكانية اختراق نظم المعلومات والاتصالات لاغتراف المعلومات أو تغير البيانات والعبث بها أو تدمير نظم المعلومات والشبكات.

## ٢ - وسائل الأمان التي يجب أن تتبع

يشمل أمن المعلومات والاتصالات استخدام وسائل تقليدية لتحقيق الأمن وكذلك وسائل حديثة غير تقليدية.

### أ - الأساليب التقليدية للأمن بالأجهزة والمنشآت :-

يشمل ذلك نظم الحراسة والأسوار والبوابات المؤمنة ووسائل الإنذار ضد الاختراق أو الحريق وتكون درجة الأمن التقليدي متناسبة مع أهمية وحساسية وموقع منشآت وأجهزة الاتصالات أو المعلومات أو الحاسبات المطلوب حمايتها ويقوم الأمن التقليدي علي عناصر فنية وإدارية و هندسية بوجود إدارات الأمن في المنشآت واستخدام الوسائل والأدوات الفنية التقليدية في الحماية والتأمين

إضافة إلى التصميم الهندسي الآمن لتلك المنشآت وصفوة القول في هذا المقام هو ما قرره عالم حديث من أن الأمن التقليدي يتمثل في الحراسة و التحصين و التشريع و التدريب و القفل والفتح .

ب - الأساليب والوسائل غير التقليدية

أن تحقيق أمن المعلومات و أمن الاتصالات في المنشأة يتمثل في ضرورة وجود نظام كفاء لإدارة المعلومات MANAGEMENT SYSTEM

OF INFORMATION وأمن المعلومات والاتصالات ويشمل ذلك : -

١ - تحديد المسؤوليات والسلطات درءاً لشيوع المسؤولية والالتزام بالنظام من الكبير والصغير .

٢ - حصول كل مستخدم لنظام المعلومات والاتصالات علي مفتاح الدخول خاص به المختلف عن مفاتيح الغير للدخول إلي النظام .

٣ - أن يكون مفتاح الدخول مكون من ستة رموز علي الأقل .

٤ - وجوب تغير مفتاح الدخول بشكل متكرر وعشوائي .

٥ - وجوب تغير مفتاح الدخول في حالة الاشتباه في معرفة غير المرخص له بمضمون المفتاح .

٦ - عدم احتواء مفتاح الدخول علي أي من الحروف الأولى لاسم المستخدم أو اختصار اسمه أو اسم شهر أو تاريخ ميلاد .

٧ - تكوين مفتاح الدخول بشكل عشوائي لتحقيق من عدم احتوائه علي تسلسل رقمي أو منطقي .

٨ - إيجاد الوسائل الفنية الآلية لتسجيل محاولات الاختراق الفاشلة للنظام وتسجيل ميعاد وتاريخ حدوثها وكذلك تحديد الوحدة الطرفية التي تمت من خلالها محاولة الاختراق .

- ٩ - مناقشة وتحليل كل محاولات الاختراق غير الناجحة واتخاذ ما يلزم لتحسين النظام .
- ١٠ - تشفير وترميز المعلومات والبيانات الحساسة .
- ١١ - تغير مفاتيح التشفير بشكل متكرر غير دوري .
- ١٢ - إسناد مهمة إدارة مفاتيح التشفير لشخصين وليس لشخص واحد باستخدام نظام ثنائي منعاً من انفراد شخص بذلك .
- ١٣ - فصل خطوط الاتصالات غير اللازمة للدخول إلي نظم الحاسبات والمعلومات .
- ١٤ - قصر توزيع المعلومات والبيانات المشفرة والحساسة علي عدد محدود ومعلوم ومرخص له في تداول تلك البيانات بقدر ما يلزم .
- ١٥ - حصر توزيع المعلومات علي الأفراد أو الأقسام التي تكون تلك المعلومات لازمة وضرورية لها للقيام بوظائف تلك الأقسام أو الأعمال دون غيرها .
- ١٦ - الحفاظ علي البيانات في بنك بيانات محدد تتوافر له الحماية .
- ١٧ - تحديد مستويات الدخول إلي النظم بشكل متعدد الطبقات .
- ١٨ - متابعة اتصالات الموظفين خارج المنشأة وكذلك تنقلاتهم وحركاتهم بين الأقسام المختلفة علي أن يكون دخول الأقسام التي تحتوي علي معلومات حساسة بترخيص كتابي خاص .
- ١٩ - في حالة استخدام المعاملات المالية المشفرة تحفظ أرقام بطاقات الاعتماد في بنوك بيانات مستقلة غير متصلة بالشبكات ويجب ألا يتضمن تداول البيانات بين الأقسام الرقم الكامل لكارت الائتمان بل آخر ٤ أرقام فقط .
- ج - الوسائل والأدوات الفنية لتوفير أمن المعلومات والاتصالات ومنها علي سبيل المثال : -



- ١ - تطبيق نظم إدارة وأمن المعلومات والاتصالات.
- ٢ - استخدام خطوط تليفونات واتصالات مأمونه .
- ٣ - استخدام وحدات تليفونات مؤمنة STU
- ٤ - استخدام قناة اتصالات آمنة.
- ٥ - استخدام تكنولوجيا الفخ الإيجابي TRAPPING POSITIVE وهو فلتر يقوم بتصيد التداخل في القنوات ويرفض ولوج غير المشتركين إلى تلك القناة.
- ٦ - استخدام تكنولوجيا الفخ السلبي TRAPPING NEGATIVE ويتم عن طريقها حجز جزء من الإشارة وبالتالي منع حصول غير المشتركين على الإشارة.
- ٧ - استخدام تكنولوجيا التشفير والترميز.
- ٨ - استخدام تكنولوجيا SSL وهي تكنولوجيا تتضمن بروتوكولاً أمنياً للإنترنت فيكون الولوج إلى النظام لمن هم مرخص لهم بذلك.
- ٩ - استخدام تكنولوجيا التوقيع الرقمي أو الإلكتروني في مهر الرسائل الإلكترونية للتحقق من نسب المستند الإلكتروني لمنشئه ومرسله.
- ١٠ - استخدام خدمات التحقق والتصديق الإلكتروني وهي خدمات متاحة عن طريق سلطات كهيئات البريد في بعض الدول أو بعض الشركات المرخص لها وهي توفر تحققاً للمتعامل في التجارة الإلكترونية من شخصية مرسل البيانات أو الطرف الآخر في العلاقات التعاقدية الإلكترونية.
- ١١ - استخدام وسائل التأكد من صحة وسلامة المراسلات الإلكترونية .
- ١٢ - استخدام البرامج المضادة للفيروسات وتحديثها بانتظام.
- ١٣ - استخدام تكنولوجيا الحوائط النارية لحماية نظم الحاسبات والمعلومات.
- ١٤ - استخدام تكنولوجيا الـ TUNNCLING لتوفير نقل مؤمن للاتصالات

عبر الإنترنت أو غيره من الشبكات.

١٥ - استخدام تكنولوجيا الكشف عن وسائل التنصت في النظم والشبكات.

١٦ - استخدام الـ **COOKIES FILE** لإراحة تلك الوسائل التي تستخدم في الدخول غير المشروع للنظام للتلصص عليه .

١٧ - استخدام تكنولوجيا العلامات المائية أو الأختام الإلكترونية الخاصة علي الوثائق الإلكترونية.

١٨ - استخدام الوسائط التكنولوجية الجديدة للدخول إلي النظم ومن ذلك مسح بصمة اليد أو قزحية أو شبكة العين.

١٩ - استخدام تكنولوجيا الإجابة والتأكيد أو تكرار التأكيد.

٢٠ - استخدام تكنولوجيا تسجيل حدوث الاتصالات.

٢١ - اللجوء لخدمات شخص ثالث مؤمن لإيداع الوثائق الإلكترونية.

٢٢ - استخدام السنقود الإلكترونية في المعاملات الإلكترونية درءاً للنصب والاحتيال والسرقة.

و أخيرا لابد من تتبلور أي محاولة من المحاولات التي تبذل سواء من مصر أو من أي دولة أو منظمة أخرى لابد من تتبلور تلك المحاولة في إطار عام يتركز حول أمن المعلومات على شبكة الإنترنت : -

**أمن المعلومات عبر شبكة الإنترنت**

## **INFORMATION SECURITY TRANS THE INTERNET**

للعمل على تحقيق أمن لكم الهائل من المعلومات الموجود على شبكة الإنترنت لابد من اتخاذ العديد من الخطوات إلا انه يمكن تقسيم تلك الخطوات إلى ثلاثة

اتجاهات هي : -

## ١ - سرية المعلومات

### SECRECY OF INFORMATION

أي ضمان حفظ المعلومات المخزنة على أجهزة الحاسبات الآلية أو تلك المنقولة عبر شبكة الإنترنت و الخطوات التي يجب اتخاذها هنا تصب جميعا في عدم إمكانية الاطلاع على تلك المعلومات إلا لمن هم مخول إليهم قانونا الاطلاع عليها فقط دون أن يتمكن أي من الغير من الاطلاع على تلك المعلومات .

## ٢ - سلامة المعلومات

### SAFETY OF INFORMATION

أي ضمان عدم تغيير تلك المعلومات المخزنة على أجهزة الحاسبات الآلية أو تلك المنقولة عبر شبكة الإنترنت و الخطوات التي يجب اتخاذها هنا تصب جميعا في عدم إمكانية تغيير تلك المعلومات إلا لمن هم مخول قانونا إليهم تغييرها فقط دون أن يتمكن أي من الغير من تغيير تلك المعلومات .

## ٣ - وجود المعلومات

### REFINDING OF INFORMATION

أي ضمان عدم حذف تلك المعلومات المخزنة على أجهزة الحاسبات الآلية أو تلك المنقولة عبر شبكة الإنترنت و الخطوات التي يجب اتخاذها هنا تصب جميعا في عدم إمكانية حذف تلك المعلومات إلا لمن هم مخول قانونا إليهم حذفها فقط دون أن يتمكن أي من الغير من حذف تلك المعلومات .

## الفهرس

رقم الصفحة	الموضوع
٥	الفصل الأول
٧	ماهية الإنترنت
٨	من يملك الإنترنت
٩	توسع الشبكة
١٠	خدمات شبكة الإنترنت
١٢	مستلزمات الاتصال بالشبكة
١٣	جرائم الإنترنت
١٣	خصائص جرائم الإنترنت
١٦	أهداف الجرائم الإلكترونية
١٧	أضرار جرائم الإنترنت
١٩	إثبات جرائم الإنترنت
٢٠	فوائد شبكة الإنترنت للأمن
٢٢	طرق ارتكاب جرائم الحاسب الآلي و الإنترنت
٢٥	الفصل الثاني
٢٧	أنواع الجرائم التي ترتكب عبر شبكة الإنترنت
٢٩	أولا : الجرائم و الممارسات الجنسية و غير الأخلاقية
٢٩	١ - المواقع الإباحية
٣٢	التكليف القانوني للجريمة
٣٤	٢ - مواقع قذف و سب و تشويه سمعة الأشخاص
٣٧	التكليف القانوني للجريمة
٣٩	٣ - الدخول إلى المواقع المحجوبة
٤٠	التكليف القانوني للجريمة

٤١	٤ - إخفاء الشخصية
٤٢	التكليف القانوني للجريمة
٤٢	٥ - انتحال شخصية الفرد
٤٤	التكليف القانوني للجريمة
٤٥	٦ - انتحال شخصية المواقع
٤٦	التكليف القانوني للجريمة
٤٦	ثانيا : جرائم الاختراق
٤٧	١ - الاختراق
٤٩	كيفية اقتحام الجهاز
٥٨	٢ - الإغراق بالرسائل
٥٩	٣ - الفيروسات
٦٢	٤ - الديدان
٦٤	التكليف القانوني للجريمة
٦٥	ثالثا : الجرائم المالية
٦٥	١ - جرائم السطو على أرقام البطاقات الائتمانية
٦٧	التكليف القانوني للجريمة
٦٨	٢ - ممارسة القمار
٦٩	التكليف القانوني للجريمة
٧٠	٣ - تزوير البيانات
٧٢	التكليف القانوني للجريمة
٧٢	رابعا : الجرائم المنظمة
٧٦	التكليف القانوني للجريمة
٧٦	خامسا : تجارة المخدرات
٧٩	التكليف القانوني للجريمة



٧٩	سادسا : غسل الأموال
٨٠	التكييف القانوني للجريمة
٨١	سابعاً : المواقع المعادية
٨٢	التكييف القانوني للجريمة
٨٣	ثامناً : جرائم القرصنة
٨٦	التكييف القانوني للجريمة
٨٦	تاسعاً : جرائم التجسس الإلكتروني
٩٠	التكييف القانوني للجريمة
٩٠	عاشراً : الإرهاب الإلكتروني
٩٢	التكييف القانوني للجريمة
٩٣	الفصل الثالث
٩٥	مكافحة الجرائم الإلكترونية
٩٦	١ - المعاهدات و المؤتمرات الدولية
٩٦	أ - معاهدة بودابست لمكافحة جرائم الإنترنت
١٠١	ب - المعاهدة الأوروبية لمكافحة جرائم الإنترنت
١٠٢	٢ - إصدار قوانين جديدة تجرم الجرائم الإلكترونية في كافة أنحاء العالم
	بحيث يكون بينها قدر كبير من التنسيق
١٠٢	أ - على المستوى العالمي
١٠٧	ب - على المستوى العربي
١١٠	٣ - التعاون الدولي
١١٤	٤ - اتحاد الشركات و الكيانات الاقتصادية في مجال حماية أمنها الإلكتروني
١١٥	٥ - المعاهدات و القوانين الخاصة بحماية حق الملكية الفكرية
١١٥	أولاً : على المستوى العالمي
١١٦	أ - معاهدة برن لحماية المصنفات الأدبية و الفنية

- ب - معاهدة تريبس - الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية ١١٧
- ج - معاهدات الويبو ١١٨
- معاهدة الويبو بشأن حق المؤلف ١١٨
- معاهدة الويبو بشأن الأداء و التسجيل الصوتي ١٢٠
- معاهدة الويبو بشأن الحماية الدولية لحق المؤلف و الحقوق المجاورة ١٢١
- ثانيا : على المستوي العربي ١٢١
- قانون حماية الملكية الفكرية الصادر بدولة الإمارات العربية ١٢١
- قانون حماية الملكية الفكرية الصادر بالمملكة العربية السعودية ١٢٤
- قانون حماية الملكية الفكرية الصادر بدولة الكويت ١٢٥
- الفصل الرابع ١٢٩
- تجربة جمهورية مصر العربية في مجال مكافحة جرائم الحاسبات و شبكات المعلومات ١٣١
- ١ - إصدار قانون حماية الملكية الفكرية المصري ١٣٤
- ٢ - تحديث القوانين السائدة إلى قوانين جديدة تجرم جرائم الإنترنت ١٣٦
- ٣ - الانضمام إلى معاهدات الدولية التي تعمل على مكافحة جرائم الإنترنت ١٤٠
- ٤ - استحداث قوانين جديدة تقن الاستخدامات الإلكترونية مثل قانون التجارة الإلكترونية و قانون التوقيع الإلكتروني ١٤٢
- ٥ - إنشاء إدارات جديدة بوزارة الداخلية تكون مسنولة عن تلك الجرائم ١٤٦
- ٦ - تحقيق الأمن المعلوماتي للكيانات الاقتصادية ١٤٩

## مكتبة سابقة المؤلفان

- ١ - الصيغ القانونية لعقود تأسيس الشركات
- ٢ - العلامات و البيانات و الأسماء التجارية
- ٣ - العقود التجارية
- ٤ - أعمال البنوك
- ٥ - الصيغ القانونية لدعاوى الشركات
- ٦ - الدفوع التجارية
- ٧ - عقد نقل التكنولوجيا
- ٨ - التوقيع الإلكتروني

## مراجع الكتاب

- داود حسن طاهر - جرائم نظم المعلومات - الرياض - أكاديمية نايف العربية للعلوم الأمنية

- عز الدين احمد جلال - أساليب التعاون العربي في مجال التخطيط لمواجهة جرائم الإرهاب - الرياض - أكاديمية نايف العربية للعلوم الجنائية  
- موقع الأستاذ / المنشاوي - على الإنترنت

WWW.MINSHAWI.COM

- موقع مجلس التعاون الخليجي

WWW.GCCSG.ORG

- موقع صحيفة ألبى بي سي

WWW.BBC.CO.UK

- محمد عادل ريان - جرائم الحاسب الآلي و امن البيانات - العربي ( ٤٤٠ )

٧٧ - ٧٣

- مؤلفنا - التوقيع الإلكتروني و حجيته في الإثبات


- الجرائم المتعلقة باستخدام البطاقات الممغنطة / الدكتور - علي عبد القادر القهوجي

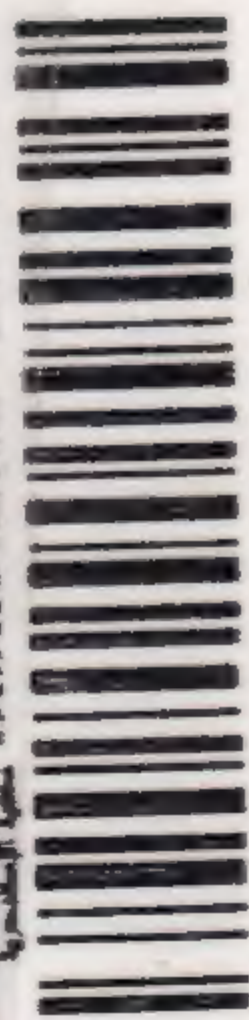
- قرار الجمعية العامة للأمم المتحدة رقم ٥١ / ١٦٢ في ١٦ / ١٢ / ١٩٩٦  
- إصدارات الأمم المتحدة - الجمعية العامة - لجنة الأمم المتحدة للقانون التجاري الدولي - الدورة الثالثة و الثلاثون - نيويورك - ٥ / ٤ / ٢٠٠٠ )







 Bibliotheca Alexandrina



0916960